Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Especificação dos requisitos de Software de análise de risco para tomada de decisão de investimentos em tecnologia da informação

Carlos Maurício de Borges Mello

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Orientador
Prof. Dr. Edgard Costa Oliveira

Brasília
2015

Universidade de Brasília — UnB
Instituto de Ciências Exatas
Departamento de Ciência da Computação
Pós-graduação em Computação Aplicada

Coordenador: Prof. Dr. Marcelo Ladeira

Banca examinadora composta por:

Prof. Dr. Edgard Costa Oliveira (Orientador) — CIC/UnB
Prof. Dr. João Carlos Félix Souza — CIC/UnB
Prof. Dr. Celso Luiz Muhlethaler Chouin — UFF

CIP — Catalogação Internacional na Publicação

Mello, Carlos Maurício de Borges.
M527e Especificação dos requisitos de Software de análise de risco para tomada de decisão de investimentos em tecnologia da informação / Carlos Maurício de Borges Mello; orientador Edgard Costa Oliveira. -- Brasília, 2015.
167 p.

Dissertação (Mestrado - Mestrado Profissional em Computação Aplicada) -- Univversidade de Brasília, 2015.

1. Gestão de riscos. 2. Tomada de decisão. 3. Requisitos de software. 4. Método AHP. I. Oliveira, Edgard Costa, orient. II Título.

Endereço: Universidade de Brasília
Campus Universitário Darcy Ribeiro — Asa Norte
CEP 70910-900
Brasília–DF — Brasil

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Especificação dos Requisitos de Software de Análise de Risco para a Tomada de Decisão de Investimentos Financeiros de Tecnologia da Informação

Carlos Maurício de Borges Mello

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Prof. Dr. Edgard Costa Oliveira (Orientador)
Faculdade UnB Gama/UnB

Prof. Dr. João Carlos Felix Souza
Departamento de Engenharia de Produção/UnB

Prof. Dr. Celso Luiz Muhlethaler Chouin
Universidade Federal Fluminense

Prof. Dr. Marcelo Ladeira
Coordenador do Programa de Pós-graduação em Computação Aplicada

Brasília, 24 de junho de 2015

Dedicatória

A Deus, pela vida e pela necessidade sempre infinita de querer aprender mais e mais.

Ao meu pai (in memoriam) e à minha mãe que sempre se preocuparam com meus primeiros estudos, desde a infância na Escola Municipal Condessa Infante até aqui, na Universidade de Brasília, no Distrito Federal. Pelo amor e disciplina e, principalmente, pela atenção dispensados em minha educação, o que contribuiu sobremaneira para que me tornasse nesse ser adulto preocupado com a educação dos demais.

À minha esposa, Kátia Mello, minha companheira de todas as horas, pela compreensão e apoio incondicional durante todo esse tempo, considerando, ainda, as inúmeras noites e madrugadas dedicadas aos estudos.

Aos meus amados filhos, Gabriel, Keyla, Maurício e Matheus, razão pela qual tudo isso foi feito. Para ser um exemplo de um crescimento profissional e pessoal e mostrar o valor do estudo e da realização acadêmica.

Aos meus irmãos, Júlio César, verdadeiramente um amigo, Marco Aurélio (in memoriam) e Tito Flávio que tudo vê e nada sabe, por ser um irmão especial.

A quatro amigos que colaboraram, em muito, para a conclusão desta pesquisa: ao Bruno Pontes com sua visão técnica, a Cácia Leal com seus conhecimentos em Língua Portuguesa, ao Fabrício Freire pela visão na área de programação e,ao Gustavo Bruzzeguez com suas colocações pontuais nas áreas orçamentária e de contratação.

Enfim, a todos que de alguma forma me fizeram chegar aqui, que me acompanharam nessa jornada pelo conhecimento, e que acreditaram em mim, quando nem mesmo eu acreditava.

A todos vocês, o meu muito obrigado!

Agradecimentos

Agradeço ao meu Orientador, Prof. Dr. Edgard Costa Oliveira, pelas observações sempre pontuais, pela amizade e acima de tudo, pela compreensão em todos os meus momentos de adversidades. Com ele, aprendi o significado de ser Educador, de ser firme e condescendente, sempre nos momentos certos. Deus o abençoe, hoje e sempre!

Ao Prof. Dr. João Carlos Félix Souza, "Prof JOCA", por me mostrar o lado bom da Educação. A alegria de lecionar e as muitas horas de conversas nos momentos que antecederam os PSP2 que me proporcionaram uma experiência única no meio acadêmico, além, é claro, de muitas coorientações para minha pesquisa.

Ao Prof. Dr. Marcelo Ladeira por ser a pessoa que é. Disciplinado, justo e principalmente, ponderado, mesmo quando em momentos de desespero, porque alunos estão sempre desesperados, conseguia nos tranquilizar, conseguia analisar, equalizar e resolver todos os problemas.

A todos os demais professores do Programa que, direta ou indiretamente, contribuíram para nossa formação: Ana Karla, Gladston, Guilherme, João Mello, Jorge Fernandes, Maristela, Sanderson e Simone Borges, que com seus ensinamentos me fez ser mais que aluno.

Aos amigos e colegas do MPCA, alguns dos quais já conhecia a tempos, e os demais onde tive a grande satisfação de tê-los conhecido.

Não podia deixar de destacar meus amigos pessoais: Democlydes, amigo de ontem, hoje e sempre, Francisco, Fausto e Nathaniel, que juntos formamos um grupo coeso e uníssono nos estudos e nas pesquisas.

Ao Prof. Dr. Celso Luiz Muhlethaler Chouin, pela forma simples que acolheu meu pedido de participação na Banca Examinadora, com competência, consideração, amizade,

apreço e constante incentivo.

Ao Departamento de Segurança da Informação e Comunicações, nas pessoas dos seguintes integrantes:

- Ao Dr. Raphael Mandarino Junior (Ex-Diretor), pela oportunidade, incentivo, apoio e autorização para a realização desta pesquisa de Mestrado;
- General de Brigada Marconi dos Reis Bezerra (Diretor), por permitir que as pesquisas fossem concluídas e pelo apoio incondicional pela minha permanência no Departamento;
- Aos demais integrantes que me auxiliaram nas pesquisas, brainstorms e, consolidação de ideias, conceitos e estratégias tão essenciais à pesquisa.

Resumo

Nos dias atuais, a Administração Pública Federal vem enfrentando um problema cada vez mais comum nas áreas de tecnologia da informação: o problema de fazer a gestão de demandas ilimitadas com recursos limitados. Os problemas são muitos e vão desde recursos humanos insuficientes, manutenção das infraestruturas de redes e, principalmente, a falta de recursos financeiros. Esse último, conduz o gestor a um dilema: ele tem a demanda de manutenção de sua infraestrutura e não tem orçamento suficiente para fazê-la. Hoje não existe um framework, um conjunto de critérios ou mesmo um sistema específico que auxilie o administrador no processo decisório para seleção dos ativos a serem escolhidos. Essa escolha acontece hoje, de forma empírica, sem um processo metodológico formal e automatizado de seleção de ativos por prioridade de investimento. Assim, este trabalho buscou identificar ferramentas de análise de riscos que pudessem auxiliar o gestor de tecnologia da informação na tomada de decisão para investimentos financeiros. A metodologia utilizada englobou atividades de pesquisas exploratórias dentro de um universo de ferramentas de uso mundial na busca de uma que atendesse o contexto da pesquisa. A pesquisa resultou na descoberta de requisitos essenciais à análise de riscos sob a óptica de investimentos. Assim, esta pesquisa identificou critérios específicos para a realização dessa análise, vem como de requisitos funcionais, requisitos de dados e regras de execução básicos para auxiliar a proposta de desenvolvimento de um software próprio, e todo este trabalho culminou com classificação desses requisitos e regras de execução para esse sistema. Por fim foi realizado um estudo de caso dentro de um universo restrito, com critérios limitados e ativos de tecnologia da informação em quantidades reduzidas para demonstrar a aplicabilidade da metodologia proposta neste tipo de análise de riscos. Essa metodologia utilizou o conceito da análise multicritério, e apresentou resultados promissores no estabelecimento de uma lista priorizando a aplicação de investimentos em tecnologia da informação, no âmbito da administração pública federal.

Palavras-chave: Gestão de risco, tomada de decisão, requisitos de software, método AHP

Abstract

Nowadays, the Federal Public Administration is facing an increasingly common problem in the areas of information technology: The problem of managing unlimited demands with limited resources. The problems are many and range from insufficient human resources, maintenance of network infrastructure and especially the lack of financial resources. The latter leads the manager to a dilemma: He has the maintenance demand of their infrastructure and he does not have enough budget. To do it. Today, there is not a framework, a set of criteria or even a specific system to assist the administrator in the decision process for selecting the assets to be worked. This selection process takes place today, empirically, without a formal and automated methodological process of selecting assets for investment priority. Thus, this study aimed to identify risk analysis tools that could help the information technology manager in decision making for investments. The methodology used comprised exploratory research activities within a universe of worldwide use tools in the search for that answer the research context. The research resulted in the discovery of essential requirements for risk analysis from the perspective of investments. Thus, this research has identified specific criteria for the purposes of analysis, comes as functional requirements, data requirements and basic implementing rules to support the proposal to develop its own software, and all this work culminated in classification of these requirements and rules implementation for this system. Finally a case study was conducted within a limited universe with limited criteria and information technology assets in small quantities to demonstrate the applicability of the proposed methodology in this type of risk analysis. This methodology used the concept of multi-criteria analysis, and presented promising results in the establishment of a list prioritizing the implementation of investments in information technology in the federal public administration.

Keywords: Risk management, decision making, software requirements, Analytic Hierarchy Process

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

1.1 Contextualização e formulação do problema

O gerenciamento de uma infraestrutura de redes de uma organização é considerado uma atividade crítica, e nos dias atuais, a diversidade de tecnologias, tanto de hardware quanto de *software*, faz com que essa atividade se destaque das demais.

Magalhães e Pinheiro [24] afirmam que, para aqueles órgãos responsáveis pelo provimento de serviços de Tecnologia da Informação (TI) obterem êxito ao programarem os seus objetivos e para que eles sejam orientados a serviço, é necessária uma mudança comportamental, que não pode se restringir à área de TI, mas também ocorrer nas áreas de negócio.

Os diversos órgãos da Administração Pública Federal (APF), em sua grande maioria, enfrentam contingenciamentos em seus recursos financeiros com relação às infraestruturas de tecnologia da informação e isso se dá, porque, embora a TI seja cada vez mais essencial a todos os órgãos, ela não é sua atividade-fim, e, por vezes, seus principais gestores não atentam para as necessidades financeiras que essas áreas demandam, ou seja, não conseguem visualizar que o planejamento estratégico da organização não pode mais ser conduzido sem que o planejamento estratégico de tecnologia da informação sejam correlacionados entre si.

Por conta dessa limitação de recurso, os administradores de TI necessitam, frequentemente, fazer escolhas difíceis, tais como definir quais tecnologias serão manutenidas, seja com suporte ou com substituição de peças ou, ainda, atualizadas.

O Tribunal de Contas da União – TCU [10] publicou em 15 de agosto de 2008, o acórdão nº 1603 apresentando diversas carências no âmbito da APF, dentre as quais, pode-se destacar a ausência de análise de riscos, principalmente, na área de TI e segurança da informação (SI).

Esse primeiro levantamento de carências de governança de TI, feito em 2007, contou com

a participação de 255 instituições e resultou no acórdão supramencionado e, diante desse cenário foi determinado que novos levantamentos dessa natureza deveriam ser realizados. O TCU [11] organizou novo levantamento, que, ao todo, avaliou cerca de 300 instituições da APF, fundamentadas, essencialmente nas normas técnicas brasileiras relativas à segurança da informação e governança de TI, no modelo Control Objectives for Information and related Technology 4.1 (Cobit 4.1) e no Programa Nacional de Gestão Pública e Desburocratização (GesPública), explorando sete das oito dimensões estabelecidas nesse programa: liderança, estratégias e planos, cidadãos, sociedade, informações e conhecimento, pessoas e, por fim, processos.

O resultado desse novo levantamento de necessidades originou o acórdão 2.308/2010-TCU-Plenário, revelando que a situação da governança de TI na APF continua bastante heterogênea, tendo evoluído em alguns pontos e em outros não. O destaque, dentre esses pontos fica com os processos de gestão de SI, de planejamento e de gestão de contratos e de serviços de TI.

A ausência da análise de riscos na área de TI, informada por 75% dos órgãos e entidades pesquisados, é um indício de que as ações de segurança não são executadas de maneira sintonizada com as necessidades do negócio dessas organizações. Isso porque, sem análise de riscos, não há como o gestor priorizar ações e investimentos com base em critérios claros e relacionados com o negócio da organização. O resultado pode ser desperdício, uso ineficaz de recursos e carência de ações prioritárias [12].

Nesse levantamento, o TCU fez comparações entre a pesquisa atual (2012) e a anterior (2010). A segurança da informação apresentou alguns indicadores negativos, conforme pode ser visto, na figura abaixo:

De acordo com Rangel [30] esse alto índice de ausência de análise de riscos apontado pelo TCU, demonstra que os órgãos da APF não possuem uma metodologia de gestão de riscos formalizada e em consequência, não possuem uma ferramenta que viabilize a gestão dos riscos relativos à SI.

Mandarino [23] ressalta a importância da elaboração de uma metodologia para avaliações de riscos em segurança cibernética, tendo em vista a necessidade de acompanhamento das informações no ciberespaço, visando à antecipação de ações preventivas em confronto aos ataques cibernéticos. Ainda de acordo com Mandarino [23], um dos objetivos do processo de avaliação da infraestrutura crítica de informação é o desenvolvimento de uma metodologia comum entre os órgãos públicos "para avaliar a vulnerabilidade das infraestruturas críticas de informação dos seus sistemas e de seus serviços".

Com base em três monografias do primeiro Curso de Especialização em Gestão de Segurança da Informação e Comunicações (CEGSIC) patrocinado pelo Departamento de Se-

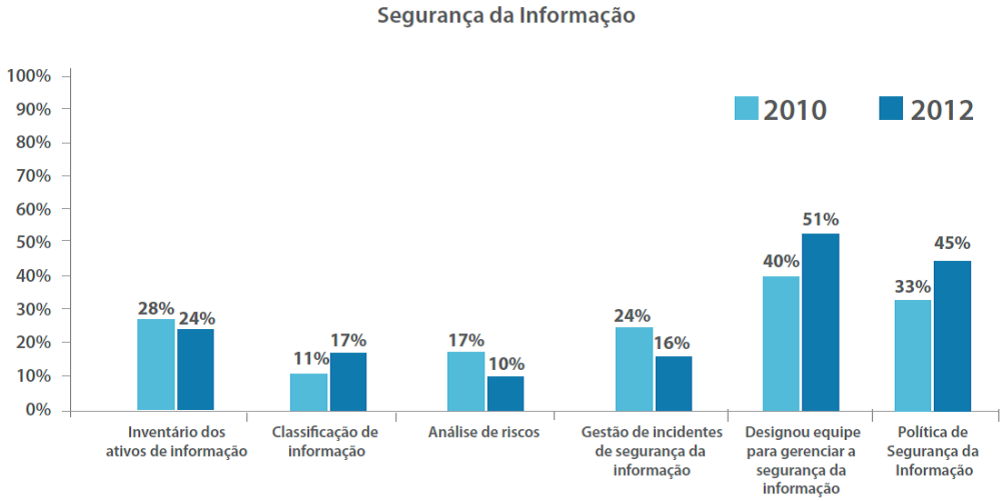

Figura 1.1: Gráfico comparativo de adoção de segurança da informação.

gurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e executado pela Universidade de Brasília (UnB), Rangel [30] apresentou um trabalho intitulado “Estudo da Metodologia de Análise de Riscos EBIOS para Aplicação na Administração Púbica Federal: Potencial Alinhamento à Legislação Brasileira", trazendo a necessidade de elaboração de uma metodologia para avaliação de risco em segurança cibernética e Mandarino [23] apresenta uma proposta de um método de análise e avaliação de risco, capaz de atender a maioria das instituições da APF, de fácil compreensão e de baixo custo. Ohtoshi [28] apresenta um estudo comparativo entre as principais metodologias e ferramentas de análise/avaliação de risco existente no mercado à época.

Como destacado anteriormente, essa ausência de análise de risco, principalmente na área de tecnologia da informação, vem preocupando cada vez mais os gestores de TI dos diversos órgãos da APF, em especial na Presidência da República, no Gabinete de Segurança Institucional.

Cada vez mais a informação, seu manuseio, guarda e transferência vem se apoiando nas tecnologias da informação, que mesmo não sendo a atividade-fim da maioria dos órgãos da APF é, sem dúvidas, a atividade-meio do qual nenhum órgão pode abdicar-se de usá-la. Toda a informação hoje circula por um mundo paralelo e transparente à maioria dos usuários, o ciberespaço e, manter essa informação segura, disponível e íntegra nesse mundo é o desafio dos gestores de infraestruturas críticas.

Dentre as diversas infraestruturas de TI existentes, aquelas que suportam as redes de informação estratégicas de alta relevância para o Governo Federal merecem um destaque específico. Todos os principais sistemas de informação ficam embarcados nessas infraes-

truturas e suas informações ficam armazenadas em equipamentos específicos com soluções robustas para recuperação de dados em caso de desastres.
Essas informações são sensíveis e, portanto, as ações sobre elas são sempre críticas e pontuais e, por conta disso, demandam dessas redes grande disponibilidade e um índice de eficiência extremamente alto.
Promover e gerir a segurança dessas infraestruturas é uma atividade complexa, pois é necessário gerir não só os ativos que suportam a solução, como também os demais equipamentos relacionados à manutenção física, como equipamentos elétricos, de proteção contra surtos de energia, de controle de acesso e ainda de refrigeração.
À medida em que os ativos dessas infraestruturas ficam mais complexos por conta da tecnologia embarcada, a margem de folga na tomada de decisões fica cada vez menor. É, portanto, imprescindível analisar os riscos de uma maneira mais ampla. O suporte de uma metodologia para o gerenciamento de risco poderá auxiliar o gerente no sentido de permitir-lhe o uso de um fator racional, lógico e dedutível em suas decisões.
Considerando que o risco existe em qualquer parte, fazer uma análise de risco desse cenário vai além da tecnologia da informação e, para administrar esses riscos é necessário basear-se não somente em tecnologias, mas em processos e pessoas.
No mercado, de um modo geral, não há uma ferramenta específica para realizar a análise de riscos em investimentos de tecnologia da informação. As ferramentas de análise de riscos preocupam-se em determinar as vulnerabilidades de equipamentos, sistemas e soluções, sob o ponto de vista técnico. Preocupam-se em levantar portas utilizadas, drivers desatualizados, patches de correção, levantamento de conformidades com normas, regulamentos, sem, no entanto, verificar problemas inerentes à contratação de uma nova solução, ou de uma atualização, à aquisição sob o ponto de vista financeiro, tão somente.
Desta forma, realizar a análise de riscos específica para essa infraestrutura é fundamental. Por não existir no mercado, ferramentas ou estruturas de análise de risco adequada para essa análise, realizar esse serviço passa a ser um desafio para o gestor de TI dos órgãos da APF.
Esse desafio significa identificar dentro das ferramentas apresentadas um conjunto de requisitos necessários para a realização dessa análise de risco. O processo de identificação irá proporcionar uma visão específica do conjunto de requisitos básicos indispensáveis a uma ferramenta que seria então, objeto para a aquisição ou da contratação de empresa especializada para o seu desenvolvimento.
Assim, esse mapeamento de requisitos destas ferramentas, auxiliará à APF:

- a subsidiar os órgãos na especificação para contratação e/ou desenvolvimento de uma ferramenta de análise e gestão de risco, mitigando assim as necessidades apontadas

pelo TCU, no tocante ao desenvolvimento de uma ferramenta pública de gestão de risco;

- a utilizar de maneira mais eficiente, os recursos financeiros para a contratação de bens e serviços de TI; e
- a reduzir as vulnerabilidades de Segurança da Informação e Comunicações (SIC) ao desenvolver um padrão básico de requisitos, permitindo a padronização, identificação e metodologia para aquisição e utilização de uma ferramenta específica para a análise de riscos dessas infraestruturas.

1.2 Justificativa

Como contextualizado antes, a escassez de recursos para investimentos de tecnologia da informação nos diversos órgãos da administração pública federal, faz com que o processo decisório ganhe importância, pois com uma margem financeira menor, as decisões têm que ser tomadas de forma mais técnica e fundamentada.
As ferramentas de análise de riscos disponíveis no mundo, preocupam-se, basicamente, em estabelecer controles de vulnerabilidades, ou verificar se as soluções de TI estão em conformidades com diversos controles baseados nos padrões COBIT, ISO, OCTAVE e NIST, por exemplo.
Estabelecer um procedimento formal para determinação de prioridades no investimento de soluções de TI baseados em critérios pré-determinados e bem ajustados passou a ser a premissa desta pesquisa.
Esse procedimento foi feito a partir da análise de riscos, com um conjunto de critérios específicos, aplicáveis aos ativos de TI e que tem forte influência no processo decisório, sob a óptica financeira.
Assim, para auxiliar nessas questões, esta pesquisa apresenta os seguintes objetivos.

1.3 Objetivos

1.3.1 Objetivo geral

Especificar um conjunto de requisitos de *software* para análise de riscos que auxilie os administradores em uma tomada de decisão de investimento em tecnologias da informação, especificamente, em ativos de redes de comunicação de dados estratégicas e de alta relevância para o governo brasileiro.

1.3.2 Objetivos específicos

Para alcançar o objetivo geral desta dissertação, os seguintes objetivos específicos foram buscados:

I Pesquisar e analisar ferramentas de gestão de risco disponíveis, visando identificar se atendem à demanda do contexto estudado, visando elicitar requisitos dessas ferramentas e realizar um estudo comparativo entre eles;

II Definir um conjunto de critérios de avaliação de riscos que sejam adotados no contexto estudado; e

III Elicitar e especificar os requisitos de um *software* para análise de riscos para a tomada de decisão de investimento em TI para o gerenciamento de redes de comunicação estratégicas e de alta relevância.

1.4 Metodologia da pesquisa

Para Gil [17], a pesquisa tem um caráter pragmático. É um "processo formal e sistemático de desenvolvimento do método científico". O objetivo fundamental da pesquisa é descobrir respostas para problemas mediante o emprego de procedimentos científicos.
Quanto à modalidade de pesquisa, do ponto de vista da sua natureza, Gil (2010) enfatiza que a pesquisa aplicada tem como objetivo gerar conhecimentos dirigidos à solução de problemas específicos. Adicionalmente, Hussey e Collins [20] corroboram, dizendo que esse tipo de pesquisa visa à aplicação de suas descobertas a um problema.
Nesse sentido, a presente pesquisa será constituída por três partes, cada uma delas diretamente relacionada aos objetivos específicos estabelecidos.
Para o estabelecimento do objetivo específico 1, foi feita uma pesquisa exploratória, qualitativa, bibliográfica e descritiva, construída segundo uma abordagem teórico-metodológica para a organização e sistematização do conhecimento sobre diversas ferramentas de análise de riscos aplicáveis ao auxílio de tomada de decisão para investimentos em TI, com foco em redes de informação estratégicas.
Stephenson [40] publicou na revista SC Magazine, um artigo intitulado "Mitigating risk as not simple as it seems" que era na verdade um preâmbulo para um trabalho desenvolvido pela equipe de pesquisa da revista sobre uma análise técnica de um grupo de ferramentas de gestão de riscos e gestão de políticas. Essa revista realizou diversos testes em um conjunto de ferramentas voltadas para a área de gestão de riscos e gestão de políticas e, inicialmente, foi feita uma pesquisa em todo o material disponibilizado pelo sítio da revista, a fim de levantar dados iniciais destas ferramentas.

Parte dessa pesquisa foi conduzida durante as atividades de monitoria desse pesquisador na disciplina de Projeto de Sistemas de Produção 2 – PSP2, do curso de engenharia de produção, da Faculdade de Tecnologia da Universidade de Brasília. Nessa atividade de monitoria, um grupo de alunos realizou uma pesquisa nos sítios das ferramentas buscando detalhes técnicos de cada uma dessas ferramentas. O resultado dessa atividade foi apresentado a análise das ferramentas de gestão de risco".
Adicionalmente a essa pesquisa exploratória, foram feitas diversas solicitações de informações complementares ao editor da revista sobre a metodologia utilizada para o estabelecimento das notas por parte da equipa da revista. Esse detalhamento também foi discriminado no item supramencionado. Assim, foi possível para o pesquisador estabelecer um conjunto de ferramentas de gestão de riscos que estão inseridas no mercado global e que efetivamente são utilizadas por empresas por todo o mundo.
A partir dessa base de dados, a pesquisa exploratória foi intensificada nos seguintes materiais:

- pesquisa exploratória no próprio sítio da revista;
- pesquisa em manuais online de algumas ferramentas;
- pesquisa nos sítios dos fabricantes; e
- pesquisa em sítios de terceiros que utilizam as ferramentas.

Para a obtenção do objetivo específico 2, "Definir um conjunto de critérios de avaliação de riscos que sejam adotados no contexto estudado" foram realizadas diversas reuniões com a equipe de planejamento e contratação do DSIC e colaboradores.
Inicialmente foram realizadas reuniões de brainstorms com a equipe de análise e planejamento orçamentário do DSIC e com a equipe técnica das coordenações para definir os parâmetros considerados essenciais numa contratação. Os critérios escolhidos foram selecionados a partir da experiência da equipe de planejamento e orçamento do Departamento e da Secretaria de Orçamento Federal – SOF.
Houve participação, de forma pontual, de membros do Exército Brasileiro, especificamente do Centro Integrado de Telemática do Exército – CITEx e do Departamento Geral do Pessoal – DGP, em reuniões ocorridas no DSIC e nas próprias instalações do Exército Brasileiro, para detalhar os critérios e estabelecer as métricas que seriam utilizadas na pesquisa. O resultado dessas reuniões pode ser visto no capítulo 4.
Para alcançar o objetivo específico 3, "Elicitar e especificar os requisitos de um *software* para análise de riscos para a tomada de decisão de investimento em TI para o gerenciamento de redes de comunicação estratégicas e de alta relevância" foram feitas análises de funcionalidades das ferramentas classificando-as de acordo com suas principais características, de acordo com o interesse da pesquisa.

As ferramentas analisadas foram então agrupadas em dois grupos: aquelas que atuam especificamente na gestão de riscos, e as que atuam na gestão de políticas.
Complementando a pesquisa, foi feito um mapeamento do processo de contratação dentro do DSIC, e para isto, foi utilizada a ferramenta de modelagem de processos Bizagi Process Modeler. Essa ferramenta foi escolhida, porque apresenta uma interface amigável e além disso, parte do processo de contratação, segue os modelos de contratação preconizados pela Secretaria de Logística e Tecnologia da Informação – SLTI, do Ministério do Planejamento, Orçamento e Gestão – MPOG que disponibilizou os modelos de forma a permitir sua adaptação e utilização no processo descrito.
Ainda nessa linha de raciocínio, foi feito outro mapeamento de processo de contratação, com foco no processo decisório. Este novo mapeamento, que representa o modelo proposto de contratação para o DSIC, auxiliou a pesquisa, permitindo o levantamento de requisitos adicionais, além daqueles que foram levantados nas ferramentas analisadas.
Após a elicitação dos requisitos, a pesquisa termina com um estudo de caso do próprio Departamento, como forma de demonstrar que a proposta é exequível e, que apresenta resultados interessantes, sob o ponto de vista financeiro.

Capítulo 2

Revisão de Literatura

2.1 Gestão de Riscos

A Associação Brasileira de Normas e Técnicas (ABNT), através da ISO GUIA 73 – Gestão de riscos – Vocabulário [1], define risco como sendo o efeito da incerteza nos objetivos, definindo ainda que efeito é um desvio em relação ao esperado, podendo ser positivo e/ou negativo. Nesse mesmo raciocínio, define, ainda que incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.

A Norma Complementar – NC 04/IN01/DSIC/GSI/PR – Gestão de Riscos em Segurança da Informação e Comunicações, do DSIC [6] define Risco (de Segurança da Informação e Comunicações) como sendo o potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

As definições de risco e incerteza, bem como a relação entre esses termos não possui um consenso quanto aos conceitos, apesar de todos os autores pesquisados admitirem a intrínseca relação que há entre risco e incerteza. Dessa forma, cabe destacar que, nesta pesquisa, será adotado para risco e incerteza, os conceitos apresentados na Norma ISO GUIA 73 – Gestão de riscos – Vocabulário, da ABNT.

A gestão de riscos utiliza como base o conceito de exposição de riscos para identificar e analisar os fatores de riscos causadores da não conformidade do processo [2].

De posse dessa visão sobre risco e incerteza, e de acordo com estudos do TCU, no Brasil, ainda não há um referencial que oriente a estruturação da gestão de riscos na administração pública federal. [12]

Nesse ano, o Tribunal de Contas da União divulgou o acórdão nr 2467, fruto de um levantamento de auditoria, que teve como objetivo a aferição do grau de maturidade de entidades públicas na gestão de risco.

O resumo desse levantamento foi classificado por setores e pode ser verificado na tabela 2.1.

Tabela 2.1: Levantamento de Maturidade em Gestão de Riscos nos órgãos da APF

Setor	**Índice Médio de Maturidade**
Elétrico	53%
Petróleo	61%
Transporte	28%
Financeiro	65%
Agências Reguladoras	31%

Analisando esse levantamento, pode-se perceber que dentro dos órgãos públicos a identificação dos riscos em processos tem se tornado uma preocupação em alguns setores, enquanto que em outros, o tema está em fase inicial.
À medida em que o tema vem se tornando relevante para alguns segmentos, há, naturalmente, um aumento significativo nos investimentos nessa área. Esse processo tem dado provimento aos administradores de subsídios essenciais à tomada de decisão, tornando-a mais precisa e assim determinar quais investimentos a empresa deve realizar, em qual equipamento, infraestrutura ou tecnologia. O risco não precisa ser hoje tão temido: administrá-lo tornou-se sinônimo de desafio e de oportunidade [35].

2.2 Gestão de Riscos de Tecnologia da Informação

Quando se fala em gestão de riscos de tecnologia da informação, pode-se dizer que os gestores de TI enfrentam um grande desafio, pois eles precisam conviver com uma grande quantidade de variáveis (hardwares, softwares) com infinitas vulnerabilidades que expõem suas infraestruturas a riscos.
Para contribuir com esse cenário negativo, esses gestores contam sempre com recursos limitados para gerenciar todo o seu ambiente de trabalho, que cada dia fica mais técnico, mais especializado e, consequentemente mais suscetível a incertezas (riscos)
Com isto em mente, a gestão de risco de TI passa então a ter um objetivo mais específico que é a busca por um ponto de equilíbrio entre investimento, priorização de recursos e segurança física ou lógica, entendendo ainda que os riscos associados à TI podem afetar o órgão, e seus objetivos estratégicos.
Essa modalidade de gestão de riscos tem algumas particularidades, como por exemplo:

- Adotar as melhores práticas de mercado para governança de segurança da informação e TI;
- alinhar a gestão de riscos com a estratégia do órgão;
- buscar soluções alternativas para tratamento dos riscos identificados; e
- obter maior controle dos investimentos de TI e assim tomar decisões com base em métricas e indicadores.

Rodrigues [31] esclarece que o Information Technology Infrastructure Library – ITIL baseia-se no ciclo de vida de serviços de TI e busca uma atividade de mensuração e melhoria de qualidade desses serviços de forma contínua, sempre tendo como foco a perspectiva do negócio e do cliente. Analogamente, essa ideia de "entrelaçar" os objetivos estratégicos de TI com os objetivos estratégicos do órgão, podem, hoje, ser facilmente estendidos para toda a TI e não somente como o ITIL sugere.
De forma complementar, o COBIT [22] entende que a aquisição é um processo que não deve ser considerado isoladamente, pois as soluções de TI existem (todas elas) para apoiar os processos de negócio. Assim, uma escolha inadequada, ou uma falha na sua manutenção, ou ainda a falta de recursos humanos capacitados pode resultar em falhas de projeto, na incapacitação momentânea das operações da organização ou ainda na redução no seu valor de negócio.
Assim, a gestão de riscos de tecnologia da informação deve, além de se preocupar com vulnerabilidades, correções e problemas técnicos, preocupar-se com os processos de contratação e/ou aquisição de soluções de TI, pois estes representam condições de incerteza, tanto quanto as vulnerabilidades técnicas em si.

2.3 O Processo Decisório

O principal obstáculo de um processo decisório, é definir qual é o problema a ser tratado. Segundo Clemen & Reilly [15], embora em geral não se tenha problemas em encontrar soluções ou problemas a resolver, às vezes, tem-se dificuldades em identificar o problema exato e então, às vezes, trata-se do problema errado.
Para Simon [37], o Processo Decisório pode ser compreendido como um processo administrativo e para ele, a decisão é um processo de análise e escolha entre várias alternativas disponíveis do curso de ação que a pessoa deverá seguir.
Após identificado o problema, o dilema do administrador é escolher qual decisão tomar diante do cenário apresentado. Assim, fica claro que a tarefa que mais caracteriza os

administradores é a tomada de decisão, porém, eles não são os únicos a decidir, pois o trabalho do executivo consiste não apenas em tomar decisões próprias, mas também em providenciar para que toda a organização que dirige, ou parte dela, tome-as também de maneira efetiva [14].

Todas as atividades humanas são, de um modo geral, permeadas pela necessidade de se tomar decisões, seja ela no nível pessoal, familiar ou até mesmo organizacional. Nesse ponto há de se destacar a maneira informal ou até mesmo intuitiva de como as decisões são tomadas. No entanto, à medida em que o mundo se torna cada vez mais dinâmico, a necessidade de melhores decisões também passou a fazer parte desse cenário e isso levou à busca de abordagens sistemáticas e estruturadas que conduzissem a um processo decisório mais satisfatório.

Devido à globalização há um crescente movimento de modificação na forma de pensar sobre a tomada de decisão. Essa nova forma de pensar traz uma nova compreensão política, que exige dos tomadores de decisão o desafio de pensar globalmente e usar, além da experiência, instrumentos de informação e comunicação que venham a colaborar no processo decisório [27].

De acordo com Gomes e Gomes [18], os modelos de apoio à tomada de decisão, em resposta à escassez dos recursos financeiros e ao ônus crescente desses recursos, fazem com que as decisões sejam tomadas com base em critérios racionais que garantam a otimização dos retornos obtidos. A introdução do risco e da incerteza nos modelos trouxe uma nova gama de informações que permitiu o aperfeiçoamento do processo decisório.

2.4 O Método AHP

O método AHP (Analytic Hierarchy Process) foi desenvolvido por Tomas L. Saaty no início da década de 70 e é o método de multicritério mais amplamente utilizado e conhecido no apoio à tomada de decisão na resolução de conflitos negociados, em problemas com múltiplos critérios.

Segundo Araújo [5], o método consiste na decomposição de um problema em uma hierarquia de critérios, que podem ser recursivamente decompostos em novos critérios até ao nível mais baixo, de forma a ficarem claros e plenamente dimensionáveis.

O método em si necessita de alguns elementos que são considerados fundamentais. Assim, esses elementos são:

- Atributos e propriedades: apresentam-se no método como um conjunto de alternativas que deve ser necessariamente comparado em relação a um outro conjunto de propriedades (os critérios).

- Hierarquia: ordenação por preferência de um conjunto de elementos que devem ser homogêneos em seus respectivos níveis hierárquicos.
- Correlação Binária: O ponto-chave do método, que é quando dois elementos são comparados baseados em uma propriedade, realizando-se então uma comparação binária, na qual um elemento é preferível ou indiferente ao outro. A métrica a ser utilizada nessa comparação é a da escala fundamental.
- Escala Fundamental: a escala de Saaty, que apresenta valores específicos para serem atribuídos prioridades a cada elemento, quando comparados na correlação binária.

Silva [36] afirma que o método AHP pode ser aplicado em duas etapas distintas:

- estruturação hierárquica do problema de decisão; e
- modelagem do método propriamente dito.

Na primeira etapa, o decisor deve efetuar a estruturação do problema, combinando os critérios selecionados segundo os diversos níveis hierárquicos necessários, para que se obtenha uma fiel representação do problema. Dessa forma, determinam-se as alternativas do problema, que serão analisadas em cada critério do nível hierárquico mais baixo.
A segunda, é a aplicação do método em si, uma vez que a hierarquia lógica dos critérios já tenha sido estabelecida, e o tomador de decisão faz, então, as comparações através de pares de critérios e finalmente, pode fazer comparações entre os elementos a serem avaliados, também, par a par, usando como referência cada um dos critérios previamente escolhidos.
Nessas comparações, o tomador da decisão deve estabelecer valores para cada par de critérios, através de uma escala numérica, desenvolvida pelo criador do método (a escala numérica de Saaty), que apresenta valores escalonados de 1 a 9 (somente números ímpares) e permitindo a utilização dos valores pares intermediários como valores de consenso. Em um esforço maior de granularidade desses valores, pode ser utilizado, ainda, valores de 0,1 (um décimo) para maiores refinamentos [33]. Os detalhes dessa escala podem ser vistos na tabela 2.2.

Tabela 2.2: Escala Saaty para medição em comparação de pares [33]

Escala	**Escala Verbal**	**Explicação**
1	Ambos elementos são de igual importância.	Ambos elementos contribuem com a propriedade,de igual forma.
3	Moderada importância de um elemento sobre o outro	A experiência e a opinião favorecem um elemento sobre o outro
5	Forte importância de um elemento sobre o outro	Um elemento é fortemente favorecido
7	Importância muito forte de um elemento sobre o outro	Um elemento é muito fortemente favorecido sobre o outro
9	Extrema importância de um elemento sobre o outro	Um elemento é favorecido pelo menos com uma ordem de magnitude de diferença
2, 4, 6, 8	Valores intermediários entre as opiniões adjacentes	Usados como valores de consenso entre as opiniões
Incremento 0,1	Valores intermediários na graduação mais fina de 0,1	Usados para graduações mais finas das opiniões

Ao término do lançamento dos valores em cada matriz, deve-se realizar o cálculo do índice de consistência [34] que é realizado através da equação ilustrada na figura abaixo.

$$CI = \frac{\lambda_{Max} - n}{n - 1}$$

Figura 2.1: Equação do Cálculo de Inconsistência [34].

Onde CI representa o índice de consistência, n, o número de critérios avaliados e λMax o valor principal de Eigen.
A fim de determinar se o CI é consistente, Saaty propôs, ainda, a chamada Taxa de Consistência (CR), que é determinada pela razão entre o valor do índice de consistência e o valor do índice de consistência aleatória (RI), também desenvolvida por Saaty [34], e que pode ser visualizado na tabela a seguir.

Tabela 2.3: Tabela de Índices de consistência aleatória [34]

N	1	2	3	4	5	6	7	8	9	10
RI	0.00	00.00	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49

Os valores de RI são fixos, conforme detalhados e, a matriz é considerada consistente se a razão proposta for menor que 10%, conforme demonstrado na figura abaixo.

$$CR = \frac{CI}{RI} < 0.1 \sim 10\%$$

Figura 2.2: Equação do Cálculo da Taxa de Inconsistência [34].

O método possui algumas variações que não serão abordadas neste estudo. Silva [36] concluiu seu estudo sobre o método AHP da seguinte forma:

> Em processos de decisão complexos, onde existem vários critérios a serem observados para uma escolha final entre diversas alternativas, o Método de Análise Hierárquica é bastante útil na estruturação do problema e modelagem matemática. A sua abordagem de divisão de critérios em hierarquias e correlação de alternativas com critérios, permite uma fácil compreensão e melhor avaliação do problema.

Considerando a importância das diversas metodologias existentes de apoio à decisão para as organizações, fica verificado que o método AHP que é baseado em uma modelagem matemática, possui grande versatilidade e flexibilidade. Sua forma de hierarquizar o problema e correlacionar os diversos critérios pode representar um diferencial na pesquisa podendo ser uma ótima alternativa para a tomada de decisão.

Capítulo 3

Estabelecimento do Contexto

Quando se fala de gestão de riscos, é preciso compreender que esse processo não ocorre num ambiente vazio. Todo e qualquer risco, não importando sua natureza, pode ser influenciado pelos ambientes que os permeia. Assim, estabelecer os contextos interno e externo dos riscos, passa a ser uma premissa para todo o processo em si.

3.1 Contexto Interno

O DSIC é um dos órgãos que compõe o GSI/PR. Sua estrutura organizacional, conforme organograma ilustrado na Figura 2, contempla as seguintes coordenações:

- Coordenação-Geral de Gestão de Segurança da Informação e Comunicações (CGGSIC);
- Coordenação-Geral de Tratamento de Incidentes de Redes (CGTIR);
- Coordenação-Geral do Sistema de Segurança e Credenciamento (CGSSC).

Além destas coordenações, o DSIC conta com 03 (três) setores de apoio: a Assessoria, o Gabinete e o Grupo de Apoio Técnico (GAT).
Dentre as diversas atribuições do Departamento, pode-se destacar as seguintes:

- Coordenar a execução de ações de segurança da informação e comunicações na administração pública federal;
- Definir requisitos metodológicos para implementação de ações de segurança da informação e comunicações pelos órgãos e entidades da administração pública federal;
- Operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal;

- Avaliar tratados, acordos ou atos internacionais relacionados à segurança da informação e comunicações;
- Coordenar as atividades relacionadas à segurança e ao credenciamento de pessoas e de empresas no trato de assuntos e documentos sigilosos; e
- Exercer outras atribuições que lhe forem delegadas pelo Secretário-Executivo.

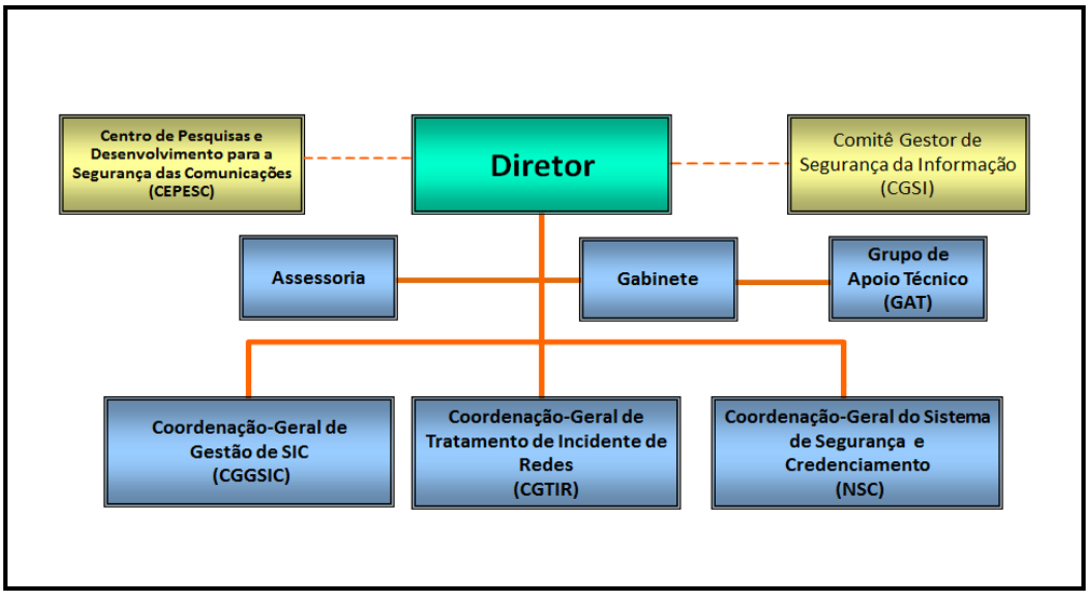

Figura 3.1: Organograma Funcional do DSIC .

Por conta dessas atribuições, o DSIC possui toda uma infraestrutura de tecnologia de informação específica que está segregada da infraestrutura da Presidência da República, por conta de sua especificidade. Todo esse aparato tecnológico é revestido de um grau de criticidade, pois os serviços que são desenvolvidos no DSIC atendem a todos os órgãos da administração pública federal.
Assim, compreender suas inter-relações internas é significativo para melhor analisar os riscos que essas infraestruturas de TI estão suscetíveis.

3.2 Contexto Externo

O DSIC, ao contrário dos demais órgãos que integram o GSI/PR, tem seu produto final voltado para o ambiente externo, o que faz com que sua relação com os demais órgãos da APF seja intensa. Por ser o órgão responsável pela normatização das ações de SIC, a forma como o próprio Departamento conduz as ações, diretrizes e metodologias visando à obtenção da disponibilidade, integridade, confidencialidade e autenticidade são exemplos

que influenciam os demais órgãos. As ações emanadas pelo DSIC têm forte impacto sobre os demais órgãos da APF.
Além disso, o DSIC possui participação fundamental no Comitê-Gestor de Segurança da Informação (CGSI), sendo suas atividades desenvolvidas em conjunto com mais de 16 órgãos da APF, que fazem desse Departamento, um expoente na área da segurança da informação e comunicações.
O DSIC possui equipes de servidores especializados para o cumprimento de suas atividades específicas das ações finalísticas de cada coordenação, além de contar com equipes adicionais responsáveis pela manutenção da vida vegetativa do Departamento, em si, ou seja, da infraestrutura essencial para o desempenho dessas atividades.

3.3 Contexto para a Tomada de Decisão baseada em Riscos

O DSIC é o órgão da APF responsável pela definição dos requisitos metodológicos para implementação da Segurança da Informação e Comunicações pelos demais órgãos. Frequentemente, o TCU tem destacado a inexistência de processos de gestão de risco em TI. Atualmente, todos os órgãos estão se vendo cada vez mais envolvidos com a evolução da Era da Informação e, essa evolução, é fortemente apoiada pelos recursos de Tecnologia da Informação e Comunicações (TIC). Assim, à medida que essas tecnologias se integram cada vez mais ao cotidiano da informação, as vulnerabilidades, os problemas e as incertezas se projetam sobre o objetivo do órgão e, demandam medidas para controle.
Todos esses problemas, são provenientes de várias fontes, dentre as quais destacam-se:

- Crescimento da dependência nos sistemas de informação baseado em tecnologias;
- limitações de segurança dos protocolos de comunicação das redes de computadores e comunicações;
- aumento do número de soluções de TI (colaboradores);
- uso de redes públicas, tais como a Internet, para o tráfego de informações;
- crescimento desordenado do comércio eletrônico;
- rápida evolução dos equipamentos usados na tecnologia; e
- desenvolvimento de novos tipos de aplicações, na busca por melhores funcionalidades e aumento de performance.

Isso posto, percebe-se que as organizações estão em constante mudança e/ou adaptação a essas novas tecnologias, que são muito dinâmicas e oferecem a cada nova implementação, a cada nova aquisição, um conjunto novo de incertezas que devem ser tratadas, ou seja, devem ser formalmente aceitas, mitigadas, eliminadas ou terceirizadas.
Para que seja feito o devido tratamento, faz-se necessário algum tipo de ferramenta que possibilite a catalogação, classificação, análise e tratamento dos riscos identificados. A APF não dispõe de uma ferramenta pública dessa natureza e somente através de esforços isolados é que cada órgão consegue uma solução para esse problema.
Além desse viés tecnológico, é necessário realizar uma análise de riscos para os ativos de TI, sob uma óptica financeira. Pois, assim como a APF não dispõe de uma ferramenta de análise de riscos tecnológicos, sequer existe uma ferramenta que verifique os riscos financeiros inerentes a cada ativo de TI, que por si só, apresentam destaques que não são mapeados, nem mensurados e, nem tampouco tratados por nenhuma ferramenta existente no mercado.
Para a execução das atribuições do DSIC, existe toda uma infraestrutura de rede própria que contém três redes de dados críticas distintas. Cada uma delas atende a um conjunto de especificidades de uma das coordenações mencionadas anteriormente.
O GAT é o setor interno que é responsável pela governança de TI no âmbito do Departamento. Dentre as suas atividades destacam-se a manutenção física e lógica dessa infraestrutura. Seus principais ativos de redes, estão, de forma sucinta, listados a seguir:

- Unidades robóticas de fita para serviços de backup;
- gabinetes para armazenamento de servidores do tipo “blade” (lâmina), com capacidade para armazenar até 16 lâminas, cada;
- soluções de segurança, do tipo firewall, que visam garantir o total controle das informações que trafegam entre as diversas redes existentes, internas e/ou externas;
- solução de segurança que atua diretamente na camada 07 do modelo de referência OSI que proporciona a detecção e bloqueio dos ataques feitos pela internet;
- equipamentos que provêm segurança física de equipamentos de rede, em ambientes que não possuam uma Sala-Cofre;
- computadores do tipo servidores para uso corporativo, somente;
- equipamentos do tipo storage para armazenamento de grandes volumes de dados;
- diversos switches de comunicação de dados;
- equipamentos de distribuição de energia para prover solução de redundância de energia para equipamentos que não possuam duas fontes de energia;

- licenças de software que fornecem uma plataforma centralizada para gerenciamento completo de ambientes virtuais; e
- equipamentos de alimentação secundários de energia elétrica.

Esses ativos possuem um grau de criticidade que varia de acordo com o serviço neles embarcado ou ainda que deles tenham absoluta dependência. A gestão desses itens demanda recursos financeiros para o estabelecimento de manutenções preventivas, preditivas e corretivas, além de atualizações, quando necessárias, ou ainda, substituição.
De uma forma geral, os recursos necessários são escassos o que obriga os gestores de TI a operar em um cenário de vulnerabilidades ilimitadas com recursos limitados, fazendo com que regras de prioridades sejam criadas para atender as limitações orçamentárias impostas a cada órgão
Isto posto, faz-se necessário o estabelecimento de um conjunto de parâmetros específicos que possam criar uma lista de prioridades lógica e eficiente para a realização dos investimentos necessários a esses ativos. Essa lista não considera os ativos por suas vulnerabilidades tecnológicas, mas sim pela criticidade de uso, combinando esta criticidade com valores estabelecidos na relação de custos entre as manutenções preventiva, preditiva e corretiva, contra o benefício que estes equipamentos podem proporcionar.
Com esse pensamento, iniciou-se um estudo voltado ao uso de uma ferramenta de análise de riscos que seja eficiente para mapear o grau de criticidade de cada ativo da rede e estabelecer parâmetros técnicos que permitam a criação dessa lista de prioridades e subsidiar assim, a tomada de decisão de investimentos financeiros na área de tecnologia de informação.
O processo de estabelecimento do grau de criticidade de cada equipamento individualizado passou por vários estágios, que vai desde o mapeamento dos ativos de rede, com descoberta de valores específicos para o estabelecimento de um contrato de manutenção, ou a substituição do equipamento.
Assim, além da contratação ser um processo complexo e demorado, a escolha sobre qual tecnologia atualizar, ou qual processo contratar deve ser feito com precisão para que não seja baseado no fator sorte.
Diversos fatores podem ser considerados para a composição desse processo de escolha. Dentre estes fatores, podem-se destacar os seguintes, mas não limitando a eles:

- base de conhecimento (Knowledge Base – KB) que o órgão possui sobre a solução;
- criticidade dos sistemas embarcados nas soluções;
- existência, por parte do fabricante, de peças de reposição;
- tempo de vida útil da solução;

- valor de atendimento “per call”[1];
- valor do desembolso mensal/anual da manutenção e/ou garantia; e
- valor financeiro do ativo.

A Tomada de Decisões baseada em riscos pode eliminar o fator sorte ao introduzir no processo de contratação um critério para escolha baseado em probabilidades conhecidas associadas em conjunto a cada um dos ativos de TI analisados. Essa atividade permitirá a construção de um modelo formalizado, capaz de ser aceito por atores que estejam envolvidos no processo decisório. Para auxiliar o processo de criação desse modelo, existe hoje no mercado, uma variedade de ferramentas de análise de riscos.
No entanto, cada uma dessas ferramentas possui um conjunto de requisitos que as fazem ser melhores em um determinado segmento de uma organização em detrimento de outro. Saber qual a ferramenta mais indicada a ser utilizada nesse cenário específico, de forma a se obter uma informação precisa para diminuir a margem de incerteza na tomada de decisão passa a ser o ponto focal desse trabalho.
A pesquisa dessas ferramentas e o levantamento dos requisitos que possuem irá ajudar na especificação do conjunto de requisitos, funcionais ou não, que seriam essenciais na determinação da ferramenta mais adequada para a realização da gestão de riscos de uma infraestrutura crítica de redes de dados.

[1]Atendimento “Per call” é a modalidade de atendimento que as empresas fazem quando o produto está fora da garantia padrão do fabricante e não dispõe da proteção de um contrato de manutenção.

Capítulo 4

Elicitação dos Requisitos das Ferramentas Analisadas

Neste capítulo serão analisadas as ferramentas selecionadas com a finalidade de elicitar seus requisitos para catalogação inicial daqueles que podem ser relevantes à pesquisa.

4.1 Introdução

Para Sommerville [39] requisitos podem ser definidos como as descrições do que o software deve fazer, os serviços que deve oferecer e as restrições ao seu funcionamento.
Os requisitos de um software geralmente são classificados em funcionais e não-funcionais, nos quais, os primeiros são identificados como sendo os serviços que o sistema deve prover ao usuário, de como o sistema deve reagir às entradas específicas e de como o sistema deve se comportar em determinadas situações. É comum um requisito funcional especificar de forma clara, o que um sistema não deve fazer.
Os requisitos não-funcionais são restrições sobre os serviços ou funções oferecidas pelo sistema. Dentro dessas restrições pode-se incluir as de tempo, as sobre o processo de desenvolvimento e as que podem ser impostas por instrumentos normativos. Em geral esses requisitos se aplicam ao sistema como um todo, em vez de um determinado recurso ou serviço do sistema.
De acordo com Gonçalves [19], a norma IEEE Std 830 [21] descreve que a especificação de requerimentos de software (Software Requirements Specifications – SRS) deve ter os seguintes atributos:

- correção;
- inequívoca;
- completa;

- consistente;
- classificada por importância e/ou estabilidade;
- verificável;
- modificável; e
- rastreável.

As especificações de cada atributo são:

1. Correção: uma SRS é correta se, e somente se, cada requisito expresso nela for aquele que o software deve cumprir.
2. Inequívoca: uma SRS é inequívoca se, e somente se, cada requisito expresso nela tiver somente uma interpretação.
3. Completa: uma SRS é completa se, e somente se, incluir todos os requisitos significantes, definição das respostas do sistema para todas as classes e rótulos completos e referências a todas as figuras, tabelas e diagramas na SRS, bem como, a definição de todos os termos e unidades de medida, quando aplicável.
4. Consistente: este atributo se refere à consistência interna. Se uma SRS não concorda com algum documento de mais alto nível, como uma especificação de requisitos de sistema, então, não é correta.
5. Classificada por importância e/ou estabilidade: uma SRS está classificada por importância e/ou estabilidade se cada requisito dela tem um identificador para indicar tanto a importância quanto a estabilidade de um requisito particular.
6. Verificável: uma SRS é verificável se e somente se, cada requisito mencionado no conjunto desse documento for verificável. A exigência é verificável se, e somente se, existir algum processo finito no qual uma pessoa ou máquina possa verificar se o produto do software atende ao requisito. Em geral, qualquer requisito ambíguo não é verificável.
7. Modificável: uma SRS é modificável se, e somente se, a sua estrutura e estilo forem tais que quaisquer mudanças nos requisitos poderão ser feitas facilmente, completamente e de forma consistente, mantendo a estrutura e estilo.
8. Rastreável: uma SRS é rastreável se a origem de cada um dos seus requisitos for claro e se puder facilitar a referência de cada requisito no desenvolvimento futuro ou documentação acessório.

4.2 Análise das ferramentas de gestão de riscos

À medida que a gestão de riscos vai ganhando importância no mercado global, diversas soluções que atuam nessa área vêm sendo desenvolvidas e disponibilizadas no mercado.
A Governança de TI cada vez mais possui um importante papel nos órgãos da administração pública federal, principalmente no que se refere à tomada de decisão. O TCU [12] vem sinalizando por anos seguidos que os órgãos da APF não possuem um modelo de governança de TI completamente implementado. Nesse cenário, a gestão e a análise de risco estão sendo deixadas em segundo plano e por conta disso, os modelos de governança de TI na APF não estão bem implementados. À medida em que os órgãos se tornam cada vez mais dependentes da TI, aprimorar o processo de governança de TI implica, necessariamente, em melhorar o processo de análise e gestão de riscos. Assim começaram a surgir nos cenários brasileiro e mundial, empresas especializadas no desenvolvimento de soluções de gestão de risco e conformidade atreladas às soluções de TI.
Stephenson [40] publicou em 2014, especificamente no mês de junho, na revista SC Magazine (for IT Security Proffessionals), que possui edições que circulam nos Estados Unidos e no Reino Unido, um estudo sobre um grupo de ferramentas que possuem características específicas para realização de gestão de riscos, dentre outras funcionalidades. O artigo, intitulado "Mitigating risk is not as simple as it seems" fez um estudo sobre um grupo de ferramentas categorizadas no grupo "risk and policy management" estabelecendo um vínculo entre ferramentas de gestão de risco e ferramentas de gestão de políticas, afirmando que uma atividade não poderia ser eficientemente conduzida sem a outra.
A proposta do artigo era apresentar como o mercado americano, em particular, está se remodelando nessa área de atuação, pois as ameaças estão se tornando cada vez mais universais e comuns a todas as empresas.
A pesquisa das ferramentas foi conduzida em um laboratório específico da própria revista, que pode então proceder à execução dos testes e avaliações necessárias. Os critérios adotados pela revista foram elencados de forma genérica sem entrar em detalhes de conformidade com nenhum normativo de gestão de risco, em específico. O foco da revista para estabelecimento dos critérios de avaliação foram os seguintes:

- recursos;
- facilidade de uso;
- performance;
- documentação;
- suporte; e

- custo-benefício.

Cada produto foi testado contra um conjunto de normas dos Laboratórios da própria revista e classificado por seus próprios méritos. Cada um dos critérios listados acima foi subdividido em outros e assim, essa subdivisão de critérios criou um universo de estudo de aproximadamente 50 tópicos gerais.
Stephenson [40] através de seu artigo, utilizou uma classificação visual baseada em estrelas. Essa classificação foi desenvolvida pelo próprio laboratório da revista, em cooperação com o Centro de Segurança Nacional e Regional na Universidade do Oeste de Michigan, e foi baseada em conjuntos de requisitos de teste específicos do produto que são desenhados pela norma de critérios comuns, a ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.
Assim, para cada produto foi dada uma classificação geral, que é determinada a partir de uma combinação das avaliações de cada um dos critérios supramencionados.
A figura 4.1 mostra um detalhamento do que representa cada um dos conjuntos de estrelas atribuídas a cada um dos critérios analisados, bem como da avaliação final dada pela revista a cada ferramenta.

Número de Estrelas	Descrição
05 Estrelas 	Excelente em todos os aspectos – um "A" no boletim do produto.
04 Estrelas 	Supera expectativas e requisitos básicos – um "B" no cartão de relatório do produto.
03 Estrelas 	Atende às expectativas da avaliação – um "C" no cartão de relatório do produto.
02 Estrelas 	Não conseguiu alcançar alguns requisitos básicos – um "D" no cartão de relatório do produto.
01 Estrela 	Seriamente deficiente – um "F" no cartão de relatório do produto.

Figura 4.1: Classificação das ferramentas de GR pela SC Magazine [40].

A equipe da revista testou cada ferramenta contra dois conjuntos de critérios. O primeiro deles foi um conjunto generalizado de tópicos que foram organizados de acordo com seis critérios principais.

Esses tópicos foram listados numa matriz de dados de teste genérica, distribuídos abaixo de cada critério e geralmente, essa matriz apresentava campos de “sim” ou “não” (na maioria dos casos) indicando a presença ou não de cada tópico.
Por fim, cada grupo de produtos teve testes individuais projetados especificamente para o grupo e cada grupo teve uma configuração de banco de ensaio exclusivo projetada para facilitar o teste dos tipos de produtos dentro do grupo.
O grupo submetido ao ensaio, “Risk & policy management” (Risco e gestão de política) possuía tópicos distribuídos em cada um dos critérios identificados anteriormente. Esses critérios foram discriminados, conforme se segue:

1. O primeiro critério “Features” (Recursos) teve como fator preponderante, na avaliação dos pesquisadores, as características que cada ferramenta possui e assim, cada ferramenta foi pontuada com base nos seguintes tópicos:

   (a) Recursos esperados;
   (b) recursos ausentes;
   (c) recursos de destaques;
   (d) recursos com pouco uso;
   (e) função dos recursos anunciados?;
   (f) banco de dados integrado; e
   (g) linguagem de scripts.

2. No segundo critério “Easy of use” (Facilidade de uso), a equipe responsável pela avaliação, considerou os seguintes tópicos:

   (a) intuitividade da interface de gerenciamento;
   (b) eficiência de tarefas;
   (c) curva de aprendizado;
   (d) integração com outros produtos;
   (e) facilidade de trabalhar;
   (f) facilidade de correção de problemas;
   (g) procedimentos de configuração definidos;
   (h) instalação intuitiva do produto;
   (i) erros encontrados;
   (j) tela de uso amigável;
   (k) automação/uso de scripts;

(l) verificação da instalação;

(m) estabilidade da instalação;

(n) conjunto de hardware e software;

(o) arquivo de log de instalação;

(p) interface de usuário intuitiva;

(q) tutoriais de usuários e processos automatizados (wizards);

(r) relatórios predefinidos; e

(s) relatórios gráficos.

3. O critério seguinte "Performance" (Atuação) teve seu subconjunto de tópicos classificados apenas como "forte" ou "fraco". Esse terceiro critério foi composto então pelos seguintes tópicos:

   (a) desempenho de performance típica;

   (b) desempenho sob ataque;

   (c) comando de resposta;

   (d) informações sobre evento.

4. O quarto critério "Documentation" (Documentação) destacou tópicos específicos aos procedimentos de uso e de instalação. No destaque abaixo estão listados os itens que compuseram esse subconjunto:

   (a) documentação compreensível;

   (b) documentação eficaz;

   (c) manuais online;

   (d) documentação de instalação;

   (e) manuais de orientação para usuário;

   (f) documentação suplementar.

5. No quinto critério de avaliação "Support" (Suporte) foram verificados os seguintes tópicos:

   (a) suporte por telefone;

   (b) downloads baseados na web;

   (c) fórum online.

6. O sexto e último critério de avaliação "Value for Money" (Custo e Benefício) foi avaliado de acordo com o seguinte subconjunto de tópicos:

(a) aquisição de sua própria empresa;

(b) preços adequados;

(c) taxas extras;

(d) atualizações incluídas

Após a análise de todos esses subconjuntos de requisitos, de acordo com Stephenson [40], há um sistema de banco de dados que agrupa todas as avaliações e calcula, de forma automática, cada um dos requisitos. Dentro desse processo há a figura de um revisor que detém a última avaliação. A esse funcionário cabe o direito de ratificar a avaliação do testador ou mudar essa avaliação. É destacado pela equipe de edição da revista que, caso o revisor julgasse a avaliação inadequada e promovesse alguma modificação, esse novo valor é o que seria publicado pela revista. No entanto, a avaliação original ficaria armazenada no banco de dados do sistema para referências futuras.
Assim as ferramentas avaliadas tiveram as pontuações obtidas pela equipe do laboratório da revista, conforme demonstrado na tabela 4.1:

Tabela 4.1: Análise das ferramentas (detalhado por requisitos)[40]

Nome	C1	C2	C3	C4	C5	C6
Acuity STREAM Integrated Risk Manager v3.1	4.00	4.00	5.00	5.00	4.00	5.00
Aegify vMarch2014	5.00	4.00	5.00	5.00	5.00	4.00
Agiliance RiskVision v7.0 (HF1)	5.00	5.00	5.00	5.00	5.00	4.00
AlgoSec Security Management Suite v6.5	5.00	4.50	5.00	5.00	5.00	4.50
Allgress Insight and Risk Manager v5	5.00	5.00	5.00	5.00	4.00	5.00
Citicus ONE vR.4.0	5.00	5.00	5.00	5.00	4.00	5.00
FireMon Security Intelligence Platform	5.00	4.75	5.00	4.00	4.00	4.75
Modulo Risk Manager v8.4	5.00	5.00	5.00	5.00	5.00	5.00
Netwrix Auditor for Active Directory	5.00	5.00	5.00	5.00	4.00	5.00
New Net Technologies Change Tracker Enterprise	5.00	5.00	5.00	4.00	5.00	5.00
Promisec Endpoint Manager	5.00	4.00	5.00	5.00	3.50	3.00
Risk Analytics as a,Service v4.1.0	4.00	4.00	4.00	5.00	4.00	4.00
RSA Archer GRC Platform,5.4 SP1	5.00	4.00	5.00	5.00	5.00	4.00
Rsam GRC Platform v 8.2	5.00	5.00	5.00	5.00	4.00	5.00
Skybox View Enterprise Suite v7.0	4.00	5.00	5.00	5.00	4.00	5.00
SolarWinds Network Configuration Manager	5.00	5.00	5.00	4.50	5.00	5.00
Titania Nipper Studio	5.00	5.00	5.00	3.50	2.50	4.00
Total Protection (ToPS) for Compliance v7.x	5.00	4.00	5.00	5.00	5.00	5.00
Tripwire Enterprise and Tripwire DataMart	5.00	5.00	5.00	5.00	5.00	4.50
TrustedAgent GRC V5.0.4	5.00	4.00	5.00	5.00	4.00	4.00
Tufin Orchestration Suite	5.00	5.00	5.00	5.00	5.00	5.00
Viewfinity Application Control	5.00	5.00	5.00	5.00	4.00	3.75

Após essas avaliações, o sistema fez ainda, uma avaliação geral, atribuindo uma única nota para cada ferramenta como pode ser visualizado na Tabela 4.2:

Tabela 4.2: Análise das ferramentas (Média Consolidada)[40]

Nome	**Nota Média**
Acuity STREAM Integrated Risk Manager v3.1	4,50
Aegify vMarch2014	5,00
Agiliance RiskVision v7.0 (HF1)	5,00
AlgoSec Security Management Suite v6.5	5,00
Allgress Insight and Risk Manager v5	5,00
Citicus ONE vR.4.0	5,00
FireMon Security Intelligence Platform	4,50
Modulo Risk Manager v8.4	5,00
Netwrix Auditor for Active Directory	4,00
New Net Technologies Change Tracker Enterprise	5,00
Promisec Endpoint Manager	4,25
Risk Analytics as a Service v4.1.0	4,00
RSA Archer GRC Platform 5.4 SP1	4,50
Rsam GRC Platform v 8.2	5,00
Skybox View Enterprise Suite v7.0	4,75
SolarWinds Network Configuration Manager	5,00
Titania Nipper Studio	4,00
Total Protection (ToPS) for Compliance v7.x	5,00
Tripwire Enterprise and Tripwire DataMart	5,00
TrustedAgent GRC V5.0.4	4,50
Tufin Orchestration Suite	5,00
Viewfinity Application Control	4,50

Com isso feito, todas as ferramentas que foram utilizadas na pesquisa foram apresentadas e detalhadas.

Para esclarecimento, convém destacar que para o levantamento das ferramentas nesta pesquisa, foi utilizada a seguinte metodologia:

- Pesquisa em diversos artigos correlatos da revista SC Magazine;
- pesquisa e análise de sítios da internet de ferramentas de gestão de riscos e gestão de políticas;

- pesquisa de manuais de utilização das ferramentas que foram obtidos através de disponibilização nos seus respectivos sítios;
- compilação dos dados apresentados no capítulo 6, com resumo dos dados do fabricante e das funcionalidades observadas de cada ferramenta selecionada;
- enfoque nos requisitos funcionais e de sistema que foram identificados nas ferramentas pesquisadas e que podem servir de fomento para o desenvolvimento de uma ferramenta específica para a pesquisa;
- contato com o fabricante da ferramenta nacional para a obtenção de informações complementares, além daquelas apresentadas no sítio da empresa;
- análise geral dos dados coletados; e
- especificação de um conjunto de requisitos essenciais ao desenvolvimento de uma ferramenta de análise de riscos para tomada de decisão de investimentos financeiros na área de TI.

A seguir, será feita uma descrição geral das ferramentas selecionadas para elicitação dos requisitos, dentre aquelas que a revista SC Magazine avaliou.

4.2.1 Acuity Stream Integrated Risk Manager V3.1

Stephenson [41] diz que esta ferramenta é orientada a riscos, que realiza monitoramento de conformidade, produção de relatórios e que pode registrar, controlar, corrigir e relatar vários padrões. Esse software é abrangente, configurável, simples de usar que automatiza processos envolvidos no gerenciamento de conformidades com as normas de gestão de riscos, incluindo a identificação de ativos, avaliação e conformidade dos riscos, entre outras, possibilitando a realização de um gerenciamento de riscos eficaz, dentro de um determinado contexto de negócios.
A ferramenta disponibiliza uma base de conhecimento das normas ISO 9001 (Sistema de Gerenciamento de Qualidade), 14001 (Sistema de Gerenciamento Ambiental), 18000 (Saúde Ocupacional e Sistema de Gestão de Segurança), 20000 (Tecnologia da Informação – Gestão de Serviços – Parte 1: Requisitos de Sistema de Gerenciamento de Serviços), 22301 (Sistema de Gestão de Continuidade de Negócios), 27001 (Sistema de Gestão da Segurança da Informação) e 31000 (Princípios e Diretrizes de Gestão de Risco), dentre outras. Essas bases de conhecimentos podem ser adquiridas avulso e não estão disponíveis em todas as versões disponibilizadas pela fabricante [25]
A ferramenta apresenta pontos específicos com relação à norma ISO 31000. A metodologia da ferramenta funciona da seguinte forma:

- automação de processos:
  - Estabelecimento do contexto do processo de gerenciamento do risco.
  - Definição dos critérios de risco:
    * a natureza e o tipo de causas e consequências que podem ocorrer e como eles serão medidos;
    * como as probabilidades serão definidas;
    * como os níveis de risco serão determinados;
    * as visões dos stakeholders;
    * o nível em que os riscos se tornam aceitáveis ou toleráveis.
    * Avaliação dos riscos:
      · identificação dos riscos através de lista de ameaças mapeadas por classes, permitindo, inclusive, o registro de novos riscos de maneira rápida e simples.
    * Análise dos riscos através de interfaces configuráveis considerando probabilidade e consequência (Vide Figura 4.2)

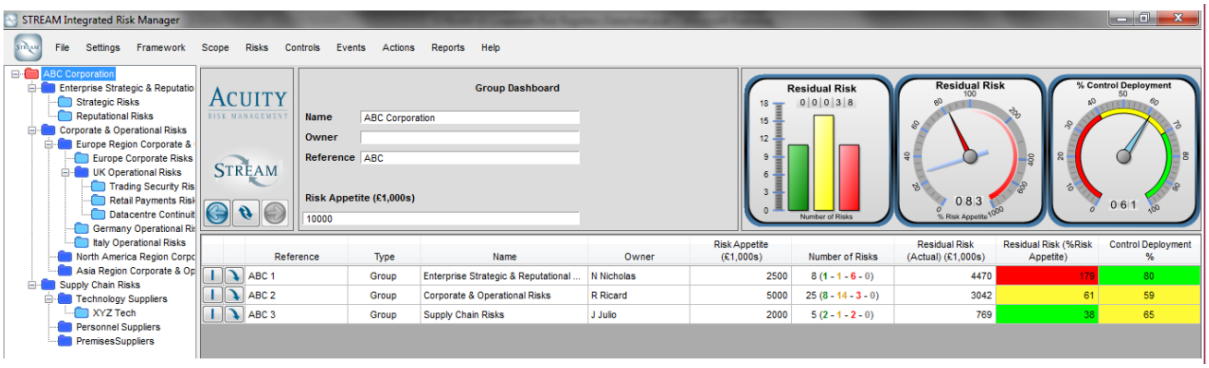

Figura 4.2: Acuity STREAM – Avaliação do Risco [25].

    * Avaliação dos riscos através de gráficos relacionados aos critérios de risco configuráveis.
    * Tratamento dos riscos através de seus mapeamentos padrão, a fim de garantir, dessa forma, uma abordagem consistente e repetitiva, permitindo, inclusive, novos registros para novos controles de risco. Esse tratamento permite, também, a preparação e implementação de planos específicos para o tratamento.
    * Monitoramento e revisão: o sistema possui uma variedade de gráficos que possibilitam o acompanhamento da evolução de todos os estágios do tra-

tamento de riscos, listando os principais riscos e os riscos residuais, dentre outros.

O manual pode incluir informações de controle de auto avaliações ou auditorias independentes, avaliações de risco – incluindo o valor da sensibilidade dos ativos de informação e probabilidade estimada de ocorrência de ameaça. Os Relatórios são gerados por gráficos 3-D, o que possibilita a transmissão de detalhes. O fabricante anuncia que o sistema é fácil de ser implantado e que possui uma curva de aprendizado com ganho rápido, o que significa dizer que, em pouco tempo, os usuários podem trabalhar com a ferramenta. Para facilitar esse ganho na curva de aprendizagem, há diversos vídeos de treinamento que já fazem parte do produto. Existem diversas modalidades de licenças que vão desde a versão gratuita até a ilimitada. Basicamente variam na quantidade de registros de riscos, níveis de empresa e classificação de ativos, que vão de 3 a 250, respectivamente, para a versão gratuita, até quantidades ilimitadas na versão mais completa. Essas licenças, exceto a gratuita, são fornecidas sob licença anual, com suporte do tipo 8/5 (oito horas por dia, cinco dias por semana) e inclui suporte o tipo Help-Desk, correção de erros e a possibilidade de fazer atualizações de software livre com a migração de dados entre as versões [25]. A figura a seguir ilustra, em detalhes, a diferença entre todas as versões disponibilizadas pelo fabricante:

	STREAM SU Free	SU Entry Subscriber	SU Small Subscriber	SU Medium Subscriber	SU Large Subscriber	SU Unlimited Subscriber
Full feature details	More Info	More Info	More Info	More Info	More Info	More Info
	Add to basket	Add to basket	Add to basket	Add to basket	Add to basket	Add to basket
Max. Risk Registers	5	5	10	25	50	Unlimited
Max. Enterprise Levels	3	3	3	4	5	Unlimited
Max. Assets	250	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Software Upgrades	✗	✓	✓	✓	✓	✓
Data Migration Services	✗	✓	✓	✓	✓	✓
Database on a server option	✗	✓	✓	✓	✓	✓
Content Uploader	✗	✓	✓	✓	✓	✓
Productivity Utilities	✗	✓	✓	✓	✓	✓
Warranty	✗	✓	✓	✓	✓	✓
Standard Support	✗	✓	✓	✓	✓	✓
Priority Support	✗	✗	✗	✗	✓	✓
License Fee per Year (GBP)	Free	GBP 295 per year	GBP 495 per year	GBP 995 per year	GBP 1,495 per year	GBP 2,495 per year

Figura 4.3: Acuity STREAM – Detalhes das versões [25].

4.2.2 Aegify vMarch2014

Segundo Stephenson [42], a ferramenta Aegify da eGestalt Technologies é uma solução baseada em assinatura, tipo software como um serviço (Software as a Service – SaaS) entregue em nuvem para monitoramento e segurança em TI, gestão de conformidade, análise de vulnerabilidade e gerenciamento de risco. Essa ferramenta atua em duas áreas específicas, uma voltada para a chamada Gestão de Postura de Segurança (Security Posture Management – SPM) e outra voltada para a gestão de risco e conformidade. A ferramenta propõe uma quebra de paradigma na forma como as empresas lidam com segurança, gestão de risco e conformidade ao oferecer uma solução fácil de usar, com uma boa relação custo e benefício. O fabricante oferece suas soluções através de uma comunidade baseada no canal provedor de serviços gerenciados.
A Aegify é extensível com suporte embutido para vários cenários específicos de regulação. Conta, hoje, com uma base de conhecimento de cerca de 800 regulações e possui um banco de dados do perfil de risco embutido que ajuda os usuários a automatizarem a gestão de riscos, aproveitando as bases de conhecimento e o conjunto de melhores práticas já documentados de normas como NIST, ISO e OCTAVE. Usando as ferramentas de interface de usuário e fluxo de trabalho, o novo módulo de gestão de risco da Aegify ajuda a definir os fatores baseados em ativos de risco e as relações entre esses fatores – aqueles que estão sendo ameaças, vulnerabilidades, impactos, probabilidade e condição predisponente [16]. Ela possui uma tecnologia de varredura em rede que proporciona a descoberta automatizada de ativos, a análise de vulnerabilidade e o monitoramento de remediação deles. Essa ferramenta também possibilita o envio de questionários online aos usuários, cujas respostas podem ser diretamente feitas na ferramenta, reduzindo a quantidade de entrada manual real necessária de uma pesquisa. O mapeamento automático de resultados da verificação para avaliações de conformidade, comentários de auditorias tornam-se muito mais fáceis e flexíveis com a auto avaliação [16].
Embora a ferramenta seja vendida como uma oferta baseada em nuvem, alguns módulos, como o SPM, devem ser executados em uma plataforma padrão Microsoft.

O módulo de política vem completo com todo o conteúdo e modelos necessários. O modelo de gerenciamento de risco da ferramenta pode ser visualizado na figura 4.4:

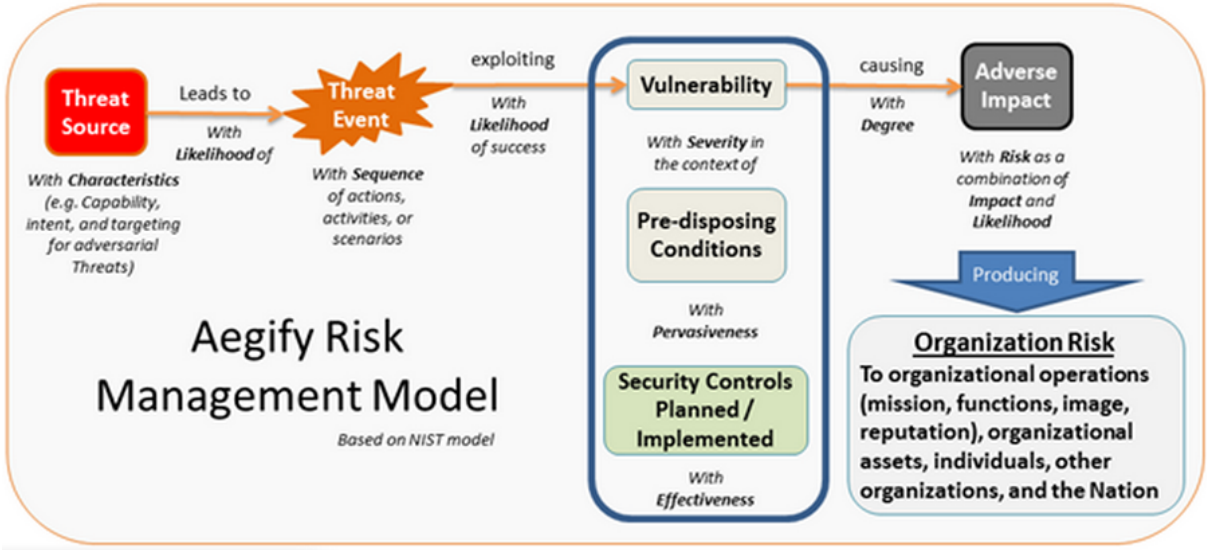

Figura 4.4: Aegify RM – Modelo de Gestão de Risco [16].

Como uma empresa americana, o padrão de gestão de riscos por ela adotado é aquele desenvolvido e distribuído pela publicação NIST SP 800-30. Existem quatro edições da ferramenta e cada uma delas é voltada para um tipo de organização, cujas edições e detalhes podem ser vistos na tabela 4.3:

Tabela 4.3: Aegify vMarch2014 – Detalhes das edições [16]

Ediçoes	**Organização a que se destina**
Ultimate	Pequenos, médios e grandes empreendimentos – múltiplas localizações de escritório – contendo equipes próprias de gestão da segurança e conformidade.
Professional	Pequenas e grandes empresas. Podem ter equipes próprias para gestão da segurança e conformidade. Esta edição oferece recursos avançados em relação à edição Standard.
Standard	Pequenas empresas – que não possuem equipes próprias de gestão da segurança e conformidade.
Community	Qualquer tamanho de organização. Ferramenta de diagnóstico com recursos limitados.

4.2.3 Agiliance RiskVision v7.0 (HF1)

Stephenson [43] diz em seu artigo que a ferramenta Agiliance RiskVision v7.0 fornece uma visão holística[2] da segurança e conformidade em uma plataforma empresarial integrada,

[2]A visão holística deriva da palavra grega "holos" que significa "todo", "inteiro", "completo".

que permite que as empresas mudem de uma abordagem orientada para ameaças reativas para uma outra, proativa, ciente de riscos. O programa traz dados de ameaças e vulnerabilidade, configuração de segurança, conformidade e avaliação de risco. Gerencia o risco organizacional, conformidade regulatória, segurança e resposta a incidentes.
A ferramenta possui vários módulos que podem ser ativados através de licenciamento adicional. Esses módulos incluem gerenciamento de conformidade, riscos corporativos e de fornecedores, ameaças e vulnerabilidades, políticas e gerenciamento de incidentes.
Ela possui um gerenciamento de risco integrado que combina as ações de gerenciamento de risco operacional com as ações de gerenciamento de risco de segurança (vide Figura 4.5), provendo para as organizações uma visão integrada de riscos, correlacionando vários cenários para fornecer uma visão unificada de risco para conformidade regulatória e auditoria de risco e risco de TI dentro da empresa. A plataforma reúne dados de ameaças e vulnerabilidades, dados de configuração de segurança, bem como o cumprimento e avaliação dos riscos. A ferramenta permite, ainda, que os usuários utilizem as informações de riscos da empresa para ajudar a fornecer visibilidade sobre o impacto nos negócios e priorizar riscos de TI e ações de correção.

Figura 4.5: Agiliance RiskVision – Gestão Integrada de Risco [3].

Essa ferramenta quebra uma prática de usar a gestão de riscos como uma consultoria contínua e passa a usar um sistema de monitoramento constante, baseado em software, de forma automatizada.
A ferramenta RiskVision da empresa possui uma construção diferenciada ao utilizar os objetivos de controle baseados nos padrões COBIT, ISO, OCTAVE e NIST para realização de suas atividades, através de um framework de mapeamento de risco, utilizado para catalogação de riscos padrões e estabelecimento de métricas de riscos comuns. Há uma grande quantidade de conteúdo previamente compilado (base de conhecimento) para políticas, avaliação, controle e elaboração de relatórios[3].

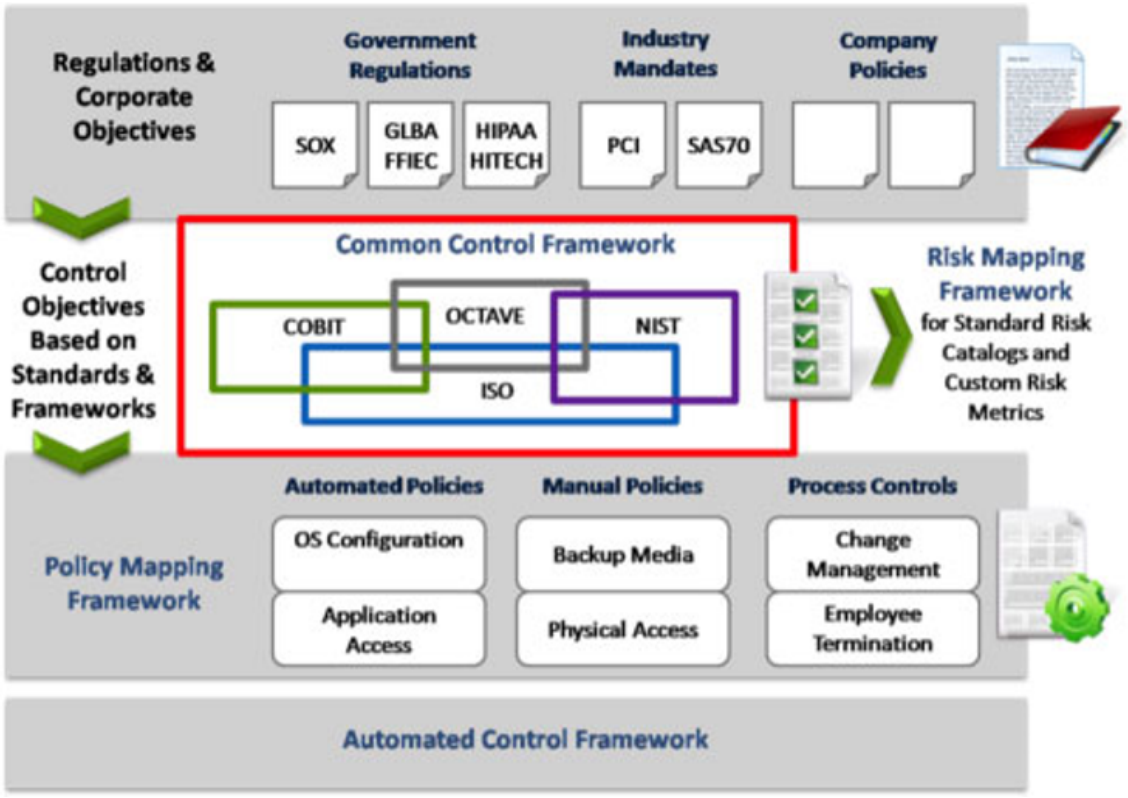

Figura 4.6: Agiliance RiskVision – Quadro de controle automatizado [3].

A ferramenta pode ser utilizada tanto como um software instalado em um equipamento quanto como uma plataforma baseada em nuvem sob demanda.

4.2.4 Allgress Insight and Risk Manager v5

Stephenson [44] afirma em seu artigo que a plataforma Allgress Insight and Risk Manager v5 é, na verdade, um conjunto de ferramentas que ajuda as empresas a agregar dados de

avaliações de segurança e conformidade e insumos técnicos e os transforma em inteligência acionável específica de risco que pode ser alinhada com os objetivos do negócio. A ferramenta combina tanto o risco empresarial quanto os riscos de tecnologia de informação em uma única plataforma modular.

O conjunto de ferramentas é construído sob uma arquitetura modular integrada e inclui avaliações, análise de vulnerabilidades, análises de riscos, gerenciamento de políticas e módulos para o gerenciamento de incidentes. Adicionalmente inclui um banco de dados centralizado que suporta a habilidade de, consistentemente, gerenciar o processo de gerenciamento de riscos de tecnologia da informação completamente e a habilidade de se integrar com soluções pré-existentes.

A ferramenta auxilia todos os líderes, da área técnica ou não, a compreenderem a postura de vulnerabilidade a riscos em uma linguagem compreensível e desta forma eles podem priorizar recursos para investimento em TI para alcançar os objetivos da empresa.

A engine da ferramenta baseia-se no framework da NIST SP 800-53, que provê um catálogo de controles de segurança para sistemas de informação do Governo federal dos Estados Unidos, exceto para aqueles sistemas relacionados à segurança nacional. No topo de tudo isso, está uma interface de usuário fácil de usar, com base, principalmente, em um modelo gráfico conduzido. A interface visual do usuário reduz a complexidade do ciclo de vida inteira da gestão de riscos e de conformidade, fornecendo automação, facilidade de uso e uma representação da informação. A interface do usuário e as ferramentas de visualização ao longo de todos os módulos são um diferencial da empresa [4].

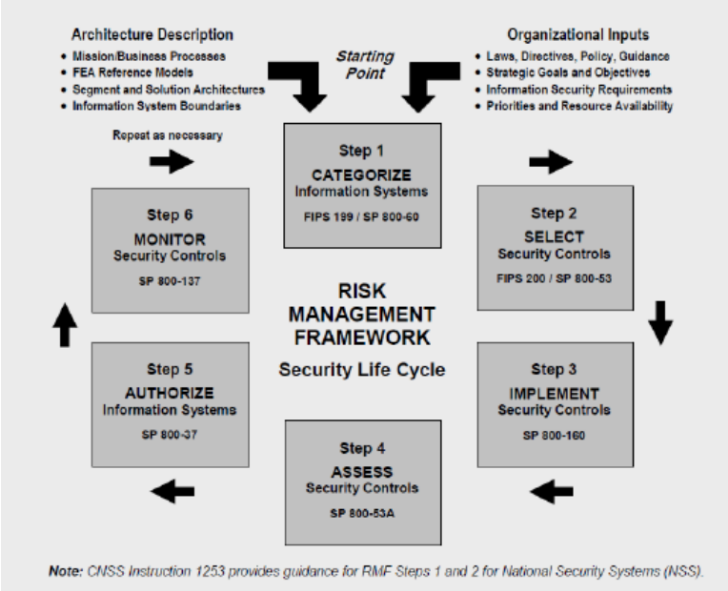

Figura 4.7: Allgress Insight and RM – NIST SP 800-53 – RM Framework [4].

A ferramenta dispõe de mapas de calor altamente visuais que fornecem a qualquer leitor uma visão imediata e intuitiva do grau de risco e de como está a postura de segurança de risco da empresa, como mostrado na figura 4.8.

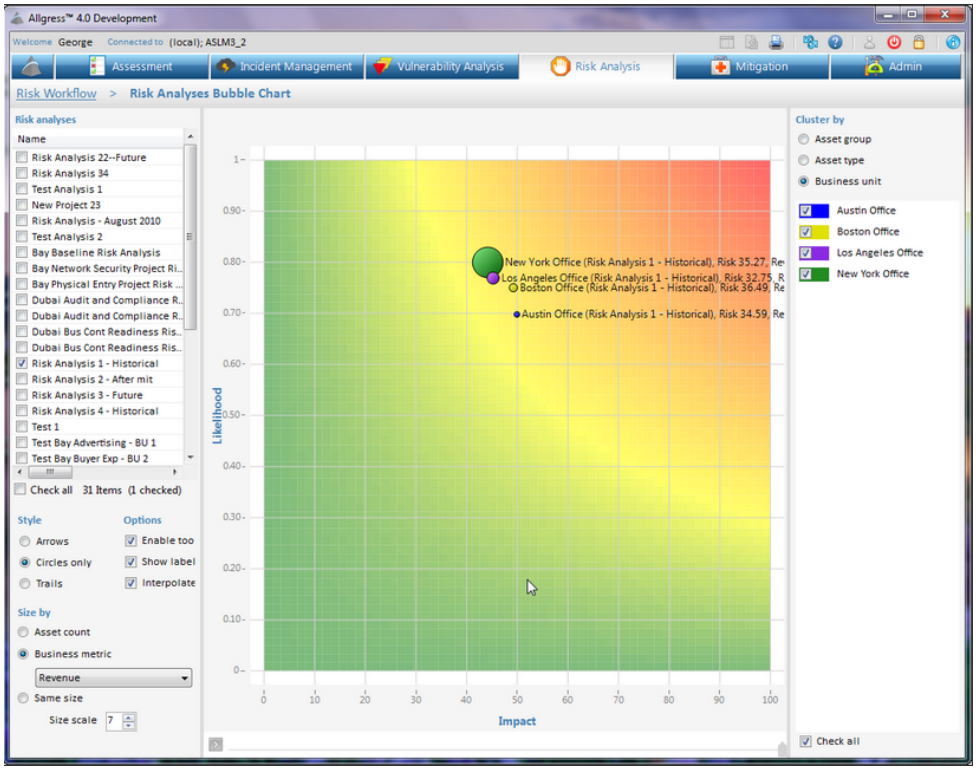

Figura 4.8: Allgress Insight and RM – Mapa de Calor [4].

4.2.5 Módulo Risk Manager v8.4

Segundo Stephenson [45], a ferramenta Módulo Risk Manager automatiza os processos de Gestão de Risco e Compliance – GRC, integrando diferentes áreas e atividades, permitindo relatórios centralizados. Ela automatiza processos para analisar, avaliar, tratar e manter o controle sobre os riscos de negócios da empresa. Essa plataforma de software também garante que os incidentes e quaisquer desvios padrões e políticas possam ser gravadas e respondidas em tempo hábil.

Dentro da ferramenta, existem vários módulos que fazem com que ela seja chamada de suíte. O gerenciamento de riscos fornece informações quantitativas e qualitativas sobre os riscos identificados e prioriza as ações, apoiando o processo de tomada de decisão enquanto os riscos são identificados. A ferramenta também ajuda as organizações a avaliar e garantir a conformidade com as normas regulamentares. A gestão de conformidade uti-

liza um MetaFramework da Módulo e suas bases de conhecimento de conformidade. Os usuários podem facilmente mapear controles em vários regulamentos, incluindo o suporte para a Sarbanes-Oxley Act of 2002 – SOX, a Payment Card Industry Data Security Standard – PCI-DSS, Health Insurance Portability and Accountability Act – HIPAA, as ISO 27001/27002, o COBIT[3] e a NIST SP 800-53, dentre outras.[26]
Os usuários também podem importar as políticas e normas internas. O módulo de gestão de políticas possibilita que as organizações administrem os esforços de gestão política enquanto avaliam a conformidade com as políticas e controles estabelecidos.
A ferramenta também pode determinar os passos que a remediação de risco, as notificações e as exceções devem percorrer. Ela integra o gerenciamento de vulnerabilidade e ameaça, além de integrar e potencializar resultados de scanners de vulnerabilidade populares para agregar e correlacionar a saída contra os bens. Esse módulo também pode ajudar a fornecer informações valiosas para priorizar as atividades de remediação.
O Módulo de Política foi atualizado para oferecer uma ferramenta de criação de políticas mais amigáveis. Há também a possibilidade de integrar o módulo de risco para qualquer fonte de informação. Mesmo se os conectores não existirem, os usuários podem ampliar os recursos, tanto quanto desejado. Relatórios e visualização foram atualizados e ainda são muito fortes.
A ferramenta foi a melhor avaliada pela revista SC Magazine e atua fortemente no mercado nacional. Possui total conformidade com a ISO 31.000, cumprindo fielmente os processos de gestão de riscos, que estão detalhados e apresentados na figura 4.9.

A ferramenta atua de forma consistente e gradativa no estabelecimento do contexto, mapeando todos os perímetros possíveis, para os diversos cenários que a organização possa ter. Versátil e adaptativa, ela se molda nos mínimos detalhes para o estabelecimento do contexto.
No processo de identificação de riscos, a ferramenta possui diversas metodologias que tem como premissa o levantamento dos riscos a que os ativos estão sujeitos. Bases de conhecimento auxiliam na execução desse processo ao simplificar as entrevistas e a coleta de dados. Muitas dessas bases geram questionários online que podem ser respondidos pelos entrevistados e suas respostas já estarão disponíveis na ferramenta, sem a necessidade de coletar e digitar, novamente, fazendo com que o tempo dessa atividade seja substancialmente reduzido.
A ferramenta dispõe de diversos coletores de evidência, cerca de 4 mil. Esses coletores atuam diretamente nos ativos tecnológicos, que podem ser software ou hardware.

[3]COBIT é um guia de boas práticas, mantido pelo Information Systems Audit and Control Association – ISACA e apresentado como framework, direcionado para a gestão de tecnologia de informação.

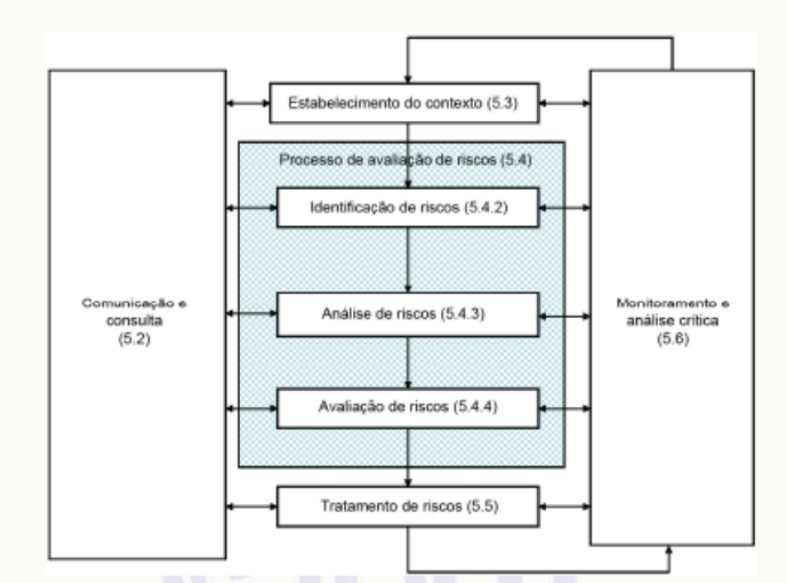

Figura 4.9: Módulo RM – Processos de gestão de riscos [2].

Stephenson [45] expõe em seu artigo que segundo a equipe de testes da Revista, a interação humana, em muitos casos, fica limitada à estimativa de relevância do ativo para a atividade da organização. Diz que o cálculo do risco é feito com base, além do parâmetro relevância, pela sua probabilidade e seu impacto, mas que estas duas últimas, estão embutidas na maioria das bases de conhecimento previamente compiladas na ferramenta. Assim, com base nos valores obtidos, os gestores podem, então, priorizar as ações possíveis de serem aplicadas aos riscos – aceitar, eliminar, mitigar ou terceirizar.
A ferramenta é bastante customizável e facilita a realização de um volume bastante diversificado de análises de riscos e, por ser de uma empresa brasileira, facilita bastante à pesquisa por uma solução que atenda ao contexto da pesquisa.

4.2.6 RSA Archer GRC Platform 5.4 SP1

Stephenson [46] afirma que a ferramenta RSA Archer GRC Platform 5.4 SP1 provê, a uma organização, uma visão consolidada de seu risco. A solução permite gerenciamento de auditorias; e avaliações de risco que podem ser feitas na abordagem tradicional, "top-down" ou ainda na modalidade "bottom-up"; ou, ainda, serem realizadas qualitativa ou quantitativamente. A solução é baseada em segurança de TI e gestão de riscos. A plataforma de GRC apresenta uma interface de usuário flexível em todos os módulos, que permite aos usuários a criação ou modificação de campos e processos para atender às necessidades do negócio.

Segundo a equipe da revista, o módulo de gestão de riscos permite abordar proativamente e endereçar os riscos à sua origem, como a reputação, as finanças, as operações e a infraestrutura de TI, tudo isso como parte de um programa de gestão de risco e conformidade. Esse é o sistema de gerenciamento central para a identificação de riscos, avaliando sua probabilidade e impacto, relacionando-os com controles de mitigação e controle da sua resolução. As ferramentas de workflow e visualização e painéis visuais são fortes.
O antigo módulo de incidente foi reformulado como o módulo de operações de segurança e fornece funcionalidade para incidentes e investigações, gestão da violação, gestão de crises e gestão de Centro de Operação de Segurança (Security Operation Center – SOC).
Com essa ferramenta, é possível documentar a hierarquia do negócio através da modelagem da hierarquia operacional que habilita os relatórios de risco e conformidade para cada nível do negócio. É possível, ainda, centralizar a infraestrutura operacional, atribuir responsabilidades e gerar relatórios diversos de maneira rápida e simples [46].
Seu módulo de gerenciamento de políticas provê um uma metodologia consistente para gerenciar o ciclo de vida das políticas corporativas e suas exceções. Sua console de gerenciamento integrada possibilita a comunicação, treinamento e rápida visualização de todas as políticas implementadas, tornando esta atividade eficiente, com uma curva de aprendizado relativamente rápida.
A ferramenta possui um centro de operações que possibilita o monitoramento e controle de pessoas, processos e tecnologia para responder de forma eficiente os incidentes de segurança e/ou violação de dados.
Por fim a console de gerenciamento de vulnerabilidades e riscos atua de forma proativa priorizando vulnerabilidades, classificando ativos e gerenciando as exceções.

4.2.7 Rsam GRC Platform v8.2

Stephenson [47] afirma em seu artigo que a plataforma Rsam GRC v 8.2 é uma ferramenta completa para o gerenciamento de riscos e inteligência de risco de segurança e que possibilita às organizações a execução de avaliação de riscos, o gerenciamento de conformidade, de ameaças e vulnerabilidades, de políticas, de atividades de remediação, de problemas, de incidentes, além de outros mais.
A plataforma centraliza a informação de fontes diversas, integrando-as em uma única console de gerenciamento. Suas soluções, por serem modulares, permitem que seja feita uma abordagem gradual na construção de projetos de gestão de risco e conformidade. Ela opera em um modelo baseado em objeto e estrutura toda a coleta de dados, processos e apresentação de relatórios em torno do conceito principal do objeto. De uma forma mais generalizada, um objeto é o alvo para a coleta e análise de dados [32].

Tendo como premissa que a escolha do framework é uma decisão crítica para o sucesso de um programa de gestão de risco e conformidade, a ferramenta está alinhada com os principais padrões disponíveis, como a ISO 27002, o COBIT e a NIST. Assim, conforme ilustrado na figura 4.10, a ferramenta fornece orientações sobre quais padrões adotar quando se busca segurança da informação, detalhes de controle ou governança de TI.

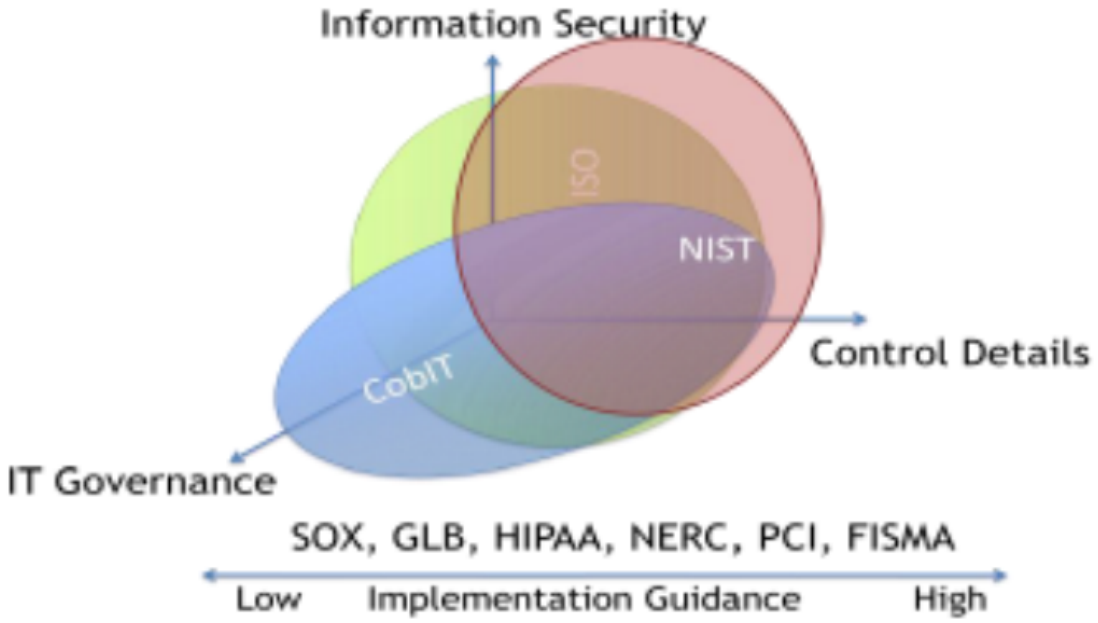

Figura 4.10: Rsam GRC Platform v8.2 – Escolha do Framework [32].

A plataforma pode ser adaptada para vários ambientes e atender às necessidades específicas de diversos órgãos com diferentes modelos operacionais.
Um bom recurso da plataforma é a habilidade de incluir qualquer usuário em avaliações e pesquisas sem a necessidade de definir esse usuário na ferramenta. Esse recurso não parece fazer muita diferença, mas economiza tempo.
Os módulos da plataforma incluem o gerenciamento de auditoria, gerenciamento de conformidades, gerenciamento de riscos empresariais, rastreio de exceções, gerenciamento de incidentes, gerenciamento de problemas, risco de tecnologia da informação, gerenciamento de políticas e risco de vendas. Todas as funcionalidades estão integradas numa única interface de gerenciamento, se a necessidade de aquisições complementares de módulos ou funcionalidades.
A ferramenta incorpora em sua base de dados uma extensa biblioteca de padrões e domínios, dentre os quais podem ser destacados: SOX, COBIT, NIST 800-53 e 53ª, PCI,

HIPAA, ISO 17788:2005/27002, e outras [32].

A figura 4.11, ilustra, de forma resumida, a forma como a ferramenta opera.

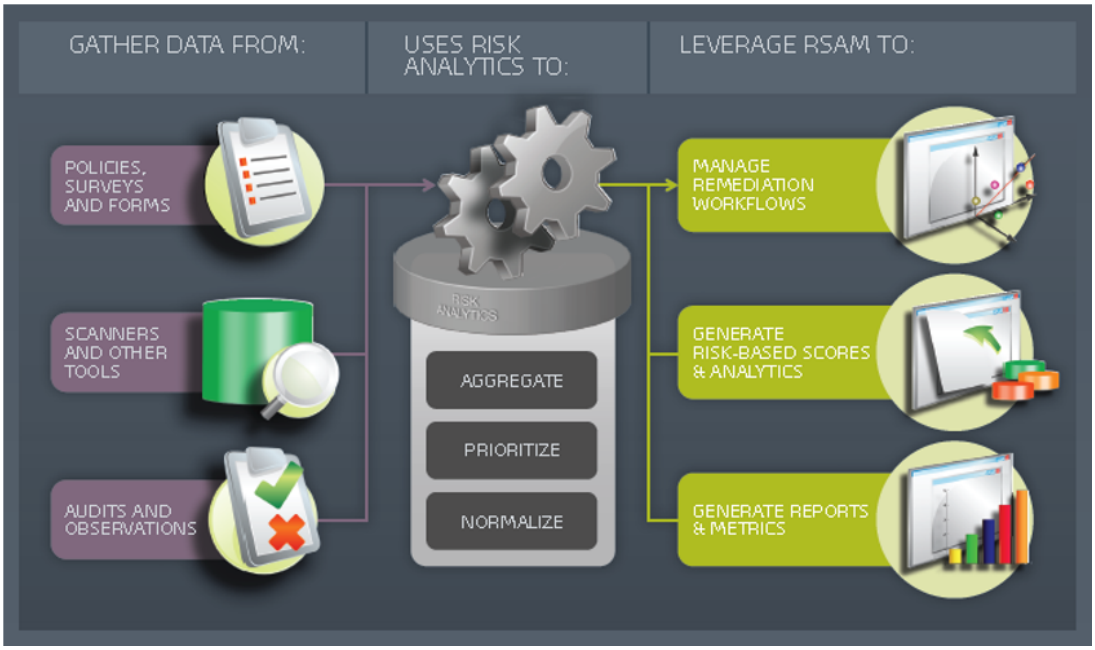

Figura 4.11: Rsam GRC Platform v8.2 – Resumo de Operação da ferramenta [32].

4.2.8 Skybox View Enterprise Suite v7.0

Stephenson [48] diz que a ferramenta Skybox proporciona uma visibilidade compreensiva da infraestrutura de segurança e que constrói um modelo virtual da rede por meio da coleta de dados de quase 80 redes e dispositivos de segurança e fontes de informação. Ela realiza a importação dos registros de configuração e dados relevantes a partir de firewalls, roteadores, IPS, scanners de vulnerabilidade, sistemas de gerenciamento de vendas, informações de ameaças e sistemas de gerenciamento de segurança. A Skybox normaliza e correlaciona os dados atualizando o modelo continuamente para que os dados sejam atuais, sem causar impactos na rede. A ferramenta desenvolve avaliações de riscos de TI e cria relatórios para mostrar PCI DSS, NIST, NERC e conformidades com outras políticas e melhores práticas. A figura 4.12 ilustra de forma genérica, os componentes dessa plataforma.

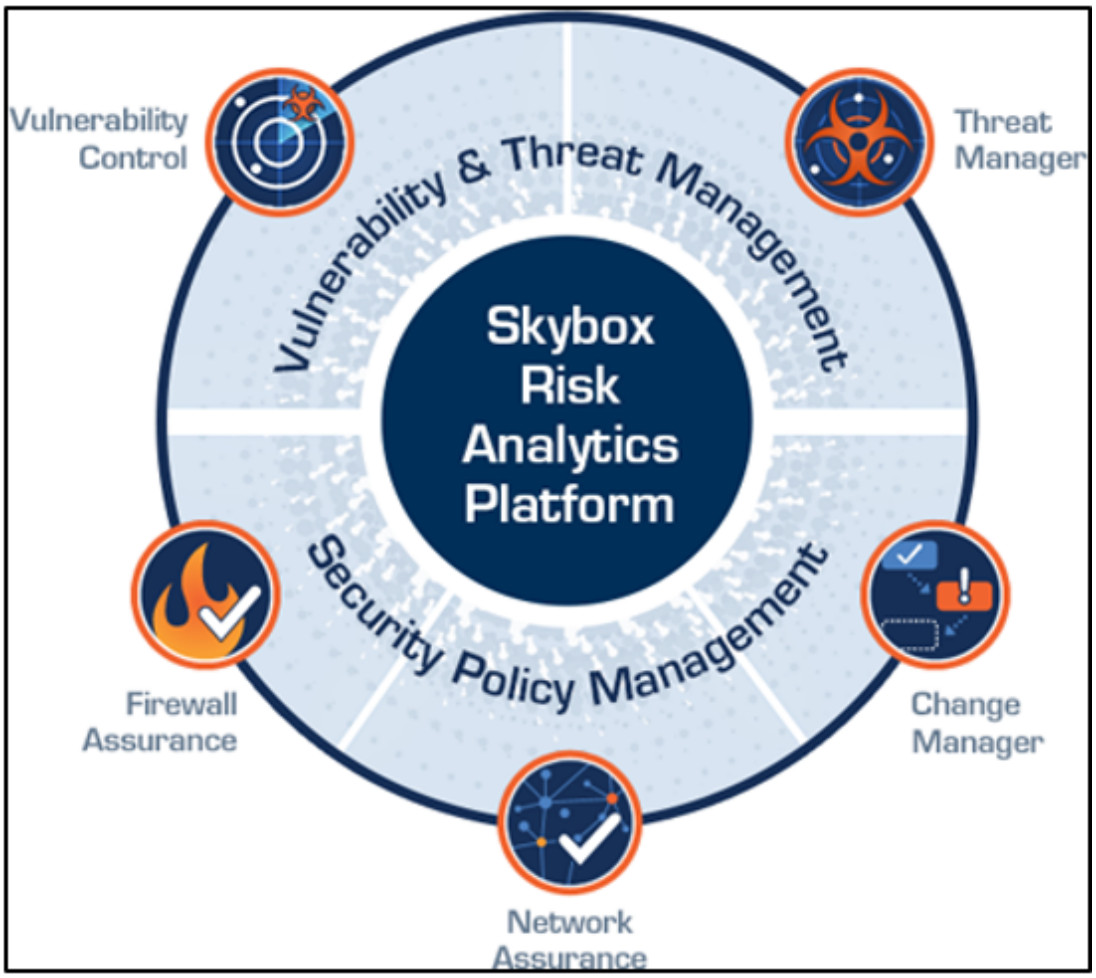

Figura 4.12: Skybox View Enterprise Suite – Componentes da Plataforma [38].

O portfólio dessa ferramenta inclui os seguintes módulos:

- Controle de vulnerabilidades: uma solução de gestão de segurança integrada que combina a descoberta das vulnerabilidades, a priorização de riscos automatizada e o fluxo de trabalho de remediação para efetivamente reduzir os riscos cibernéticos.
- Gerenciamento de ameaças: avalia as últimas informações de ameaças contra o contexto de ativos de uma organização, com destaque para os impactos potenciais de negócios, priorizando automaticamente as ameaças vitais.
- Garantia de políticas de firewall: examina as regras de firewall e configurações automaticamente para manter a rede segura, otimizada e em conformidade com regulamentos e políticas com o mínimo esforço.
- Garantia de políticas de rede: fornece visibilidade completa da topologia da rede e apresenta respostas rápidas para a configuração de dispositivos de rede em segundos.

- Gerenciamento de mudanças: automatiza o fluxo de trabalho do processo de gestão de mudança em um firewall.

A funcionalidade Skybox Controle de Vulnerabilidade descobre vulnerabilidades diariamente, avalia automaticamente o risco do negócio e prioriza atividades de correção dentro do contexto de sua rede [38].
A solução proporciona uma visão consciente do contexto da rede e dos riscos que impulsionam grandes vulnerabilidades em escala empresarial e gerenciamento de ameaças, gerenciamento de firewall e monitoramento de conformidade, conforme ilustra a figura 4.13.

Figura 4.13: Skybox View Enterprise Suite – Painel de controle de riscos [38].

Esse painel de controle oferece uma visão centralizada do processo de avaliação de vulnerabilidade inicial, incluindo acesso rápido a dados de vulnerabilidade recolhidos.
O Centro de análise utiliza sofisticados mecanismos de análise de riscos para eliminar dados de vulnerabilidade irrelevantes e pode fornecer um quadro preciso de vulnerabilidades priorizado por risco.
Dentro desse cenário de gerenciamento de vulnerabilidades, a ferramenta apresenta, ainda, o centro de remediação, que proporciona uma boa maneira de gerenciar o ciclo de vida

de cada vulnerabilidade.
Esse centro equaliza numa única visão todas as ameaças, provendo, de forma consistente, uma visão consolidada de todos os alertas das ameaças, bem como todos os boletins correlatos. Numa segunda estância, a ferramenta classifica as ameaças pelo impacto potencial que elas podem ter no negócio, classificando ainda, os esforços para sua remediação. Por fim, essa console recomenda a remediação adequada para cada ameaça, automatizando ainda, o processo de rastreio das soluções escolhidas [38].

4.2.9 TrustedAgent GRC v5.0.4

Stephenson [49] informa que a plataforma TrustedAgent GRC V5.0.4 é uma ferramenta de gerenciamento de riscos de TI modelada a partir da estrutura de gestão de risco estabelecida pela NIST SP 800-37 e que engloba atividades de definição, classificação, planejamento, implementação, avaliação, gerenciamento, autorização e fiscalização dos riscos.
Essa solução fornece uma visão empresarial que busca a integração, a padronização e a melhoria dos processos de GRC que existem no órgão.
A ferramenta é compatível com outros frameworks padrão de gestão de segurança da informação, como a ISO 27001, COBIT, SOX, PCI, Federal Financial Institutions Examination Council – FFIEC, NERC, NIST, HIPAA e outros, automatizando a utilização de TI, os riscos e os processos de conformidade, incluindo a autorização, o cumprimento, o gerenciamento de políticas e a gestão de incidentes, tudo isso de forma centralizada em uma console [50].
A ferramenta é capaz de estabelecer o contexto de um órgão, agrupando os metadados (ativos) em até três classes distintas: sistemas, sítios e programas. A classe de sistemas armazena ativos do tipo aplicações; a classe sítio, datacenters com localização física; e por fim, a classe programas, para políticas e procedimentos. Isso pode ser visto na figura 4.14.

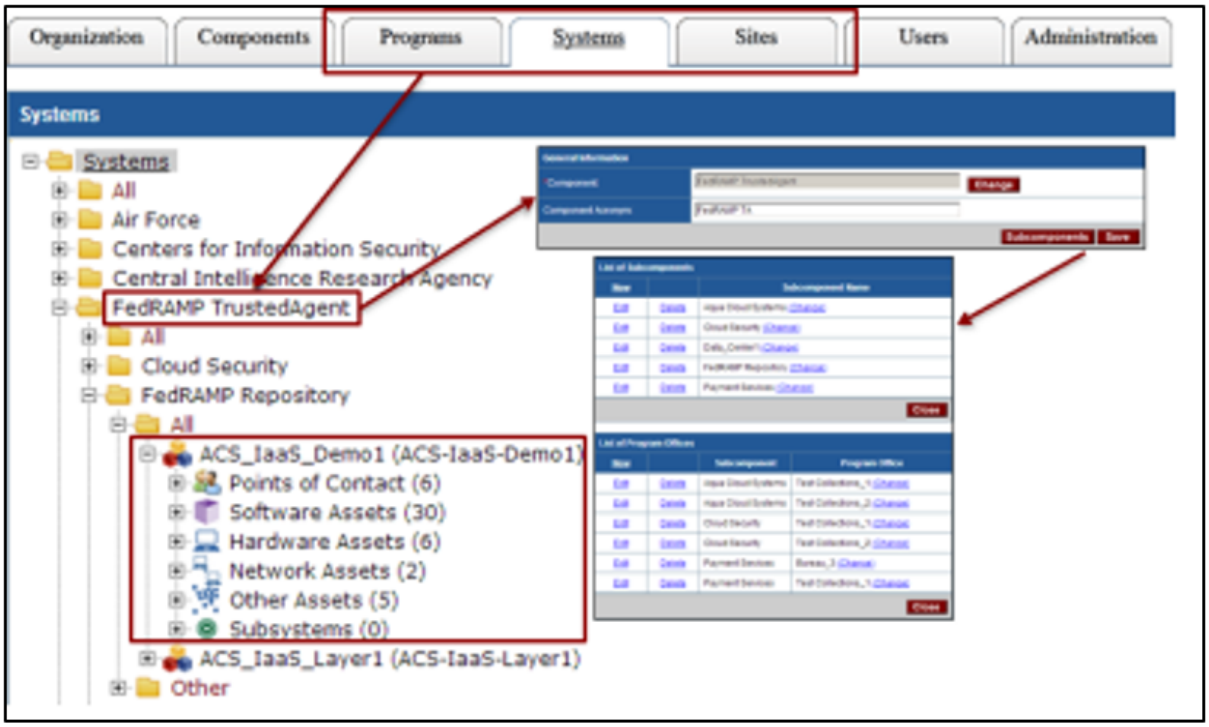

Figura 4.14: TrustedAgent GRC – Hierarquia Organizacional [50].

Uma vez que a entidade básica, as definições de negócios e as definições de ativos estejam criadas, a ferramenta comunica e controla a aderência às políticas e procedimentos, realizando revisões de risco às normas específicas, identificando áreas de risco expostos e realiza o gerenciamento das atividades de remediação e mitigação do risco.
Os riscos identificados a partir de auditorias, avaliações de controle e dados de vulnerabilidade são correlacionados, geridos e relacionados ao ativo afetado. A ferramenta oferece vários métodos para determinar qual o nível de risco, as ações corretivas e o tratamento de riscos apropriados. Essas conclusões podem levar a uma ação corretiva.
Os relatórios podem ser criados, podendo acrescentar a eles os comentários técnicos que podem ajudar o sistema. Eles apresentam um padrão bem definido para os documentos, nos quais há inúmeros relatórios padrão disponíveis, além de relatórios que podem ser montados usando algumas de suas ferramentas.

4.3 Seleção das ferramentas

Após a análise das ferramentas, apresentadas no item anterior, foi verificado pelo pesquisador que dentre as ferramentas estudadas, apenas duas delas receberam avaliação máxima pela equipe de análise da revista em todos os tópicos analisados. As ferramentas são a Modulo Risk Manager v8.4 e a Tufin Orchestration Suite, conforme pode ser observado na tabela 4.x.

Tabela 4.4: Destaque das Maiores Notas atribuídas às ferramentas analisadas[40]

Nome	C1	C2	C3	C4	C5	C6
Acuity STREAM Integrated Risk Manager v3.1	4.00	4.00	5.00	5.00	4.00	5.00
Aegify vMarch2014	5.00	4.00	5.00	5.00	5.00	4.00
Agiliance RiskVision v7.0 (HF1)	5.00	5.00	5.00	5.00	5.00	4.00
AlgoSec Security Management Suite v6.5	5.00	4.50	5.00	5.00	5.00	4.50
Allgress Insight and Risk Manager v5	5.00	5.00	5.00	5.00	4.00	5.00
Citicus ONE vR.4.0	5.00	5.00	5.00	5.00	4.00	5.00
FireMon Security Intelligence Platform	5.00	4.75	5.00	4.00	4.00	4.75
Modulo Risk Manager v8.4	**5.00**	**5.00**	**5.00**	**5.00**	**5.00**	**5.00**
Netwrix Auditor for Active Directory	5.00	5.00	5.00	5.00	4.00	5.00
New Net Technologies Change Tracker Enterprise	5.00	5.00	5.00	4.00	5.00	5.00
Promisec Endpoint Manager	5.00	4.00	5.00	5.00	3.50	3.00
Risk Analytics as a,Service v4.1.0	4.00	4.00	4.00	5.00	4.00	4.00
RSA Archer GRC Platform,5.4 SP1	5.00	4.00	5.00	5.00	5.00	4.00
Rsam GRC Platform v 8.2	5.00	5.00	5.00	5.00	4.00	5.00
Skybox View Enterprise Suite v7.0	4.00	5.00	5.00	5.00	4.00	5.00
SolarWinds Network Configuration Manager	5.00	5.00	5.00	4.50	5.00	5.00
Titania Nipper Studio	5.00	5.00	5.00	3.50	2.50	4.00
Total Protection (ToPS) for Compliance v7.x	5.00	4.00	5.00	5.00	5.00	5.00
Tripwire Enterprise and Tripwire DataMart	5.00	5.00	5.00	5.00	5.00	4.50
TrustedAgent GRC V5.0.4	5.00	4.00	5.00	5.00	4.00	4.00
Tufin Orchestration Suite	**5.00**	**5.00**	**5.00**	**5.00**	**5.00**	**5.00**
Viewfinity Application Control	5.00	5.00	5.00	5.00	4.00	3.75

A primeira ferramenta, a Modulo Risk Manager v8.4, foi considerada como sendo uma ferramenta poderosa, versátil e capaz de entrar em operação em um órgão sem muito esforço. A equipe da revista considerou essa ferramenta como a melhor opção de compra para entidades que necessitassem realizar atividades de gestão de riscos e conformidade.

A segunda, apesar de ser igualmente bem avaliada, não possui o foco voltado para ações de análise de risco e sim para ações em gestão de políticas. A pesquisa conduzida pela equipe da revista foi realizada em um grupo de ferramentas de gestão de riscos e gestão de políticas. As duas ferramentas estão em grupos distintos e receberam nota máxima, em cada um dos grupos a que pertencem.
As outras ferramentas, as excluídas da pesquisa, estão apresentadas na tabela 4.5, inclusive com uma breve descrição da principal funcionalidade delas, que foi, basicamente, o motivo que levou as suas exclusões da etapa de elicitação de requisitos.

Tabela 4.5: Ferramentas excluídas da pesquisa – Justificativas

Nome	**Justificativas**
AlgoSec Security Management Suite v6.5	Apresenta foco em gestão de políticas.
Citicus ONE vR.4.0	Apresenta foco em análise de risco organizacional, sem foco na TI.
FireMon Security Intelligence Platform	Apresenta foco em gestão de políticas.
Netwrix Auditor for Active Directory	Apresenta foco em processos de auditoria em infraestrutura de AD.
New Net Technologies Change Tracker Enterprise	Apresenta foco em processos de conformidade e auditoria de mudanças.
Promisec Endpoint Manager	Apresenta foco em gestão de conformidade de ativos de rede.
Risk Analytics as a Service v4.1.0	Apresenta foco em análise de risco em BigData - Dados em geral.
SolarWinds Network Configuration Manager	Apresenta foco em gestão de conformidade de ativos de rede.
Titania Nipper Studio	Apresenta foco em gestão de conformidade de ativos de rede.
Total Protection (ToPS) for Compliance v7.x	Apresenta foco em processos de auditoria em infraestrutura de AD.
Tripwire Enterprise and Tripwire DataMart	Apresenta foco em processos de auditoria em infraestrutura de TI.
Tufin Orchestration Suite	Apresenta foco em gestão de políticas para ativos de rede.
Viewfinity Application Control	Apresenta foco em gestão de políticas de uso de aplicativos em redes.

4.4 Requisitos elicitados

Como descrito antes, no decorrer da pesquisa dessas ferramentas, foi feito um levantamento nos sítios de todos os fabricantes, na procura por informações complementares, buscando contatos, manuais e representações no Brasil. Os resultados serão apresentados a seguir.
Para essa etapa foram elencados requisitos específicos para as ferramentas, com foco na gestão de riscos. Assim, requisitos considerados necessários foram aqui listados para observação e utilização futura:

- estabelecimento do contexto;
- cadastro de ativos;
- cadastro de atributos de ativos;
- atribuição de responsabilização por ativo (para stakeholders);
- cadastro de critério para análise de risco;
- customização de matriz de risco;
- exportar relatórios em planilhas eletrônicas;
- importar relatórios de planilhas eletrônicas;
- confecção de matriz de comparação de critérios (Método AHP);
- criação de matriz de comparação de ativos por critério (Método AHP);
- criação de relatórios por grupo de ativos;
- criação de relatórios de análise de risco;
- instalação em plataforma Windows;
- instalação em plataforma Linux;
- possuir rotinas de backup e restauração;
- integração com o Active Directory;
- integração com o LDAP.

Nos próximos tópicos serão detalhados esses requisitos elicitados das ferramentas estudadas.

1. **Estabelecimento do contexto:** Mapeamento de riscos e dos ambientes que podem influenciá-los, definindo os critérios e o escopo da gestão.

2. **Cadastro de ativos:** O cadastro de ativos tem como finalidade permitir que a associação entre um componente de ativo e uma base de conhecimento possam ser utilizadas para a medição de risco. De fato, esse cadastro funciona como um registro de todos os detalhes técnicos relevantes que podem ser utilizados em etapas posteriores da análise em si.

3. **Cadastro de atributos de ativos:** Esse requisito complementa o requisito anterior. O esperado nas ferramentas é que no "cadastro de ativos" haja um conjunto de atributos a ser preenchido para uso posterior. A ideia é de que a ferramenta possibilite a criação de novos atributos, de acordo com a especificidade dos ativos e da análise de risco.

4. **Atribuição de responsabilização por ativo (para stakeholders):** Esse requisito destina-se à seleção de uma pessoa, que deve estar previamente cadastrada no sistema, que deve responder pelo ativo. Essa pessoa será a responsável por fornecer as informações relacionadas aos atributos dos ativos, principalmente no tocante ao cálculo do risco.

5. **Cadastro de critério para análise de risco:** O cadastro de critérios tem como finalidade permitir que sejam adicionados critérios específicos à análise de risco. Entende-se que essa análise pode ser feita com foco específico para cada fim. O objetivo desse critério é, portanto, a inserção de critérios além daqueles pré-existentes na ferramenta.

6. **Customização de matriz de risco:** A matriz de riscos é um instrumento que visa ao mapeamento de todos os riscos catalogados de acordo com seus respectivos níveis de probabilidade, impacto e severidade propostos, permitindo, assim, que os riscos mais críticos sejam rapidamente identificados através de uma forma visual. Customizar essa matriz de riscos significa ajustar a forma como os riscos serão identificados. Significa que o usuário poderá criar matrizes de riscos específicas a cada cenário, se for o caso.

7. **Exportar relatórios em planilhas eletrônicas:** Exportar relatórios em planilhas eletrônicas é um requisito que facilita a seleção, ordenação e/ou consultas em relatórios extensos. Desenvolver diversos tipos de consulta em um relatório exige um esforço computacional da ferramenta. Ao transportar o conteúdo de um relatório para uma planilha eletrônica, abre-se um conjunto de possibilidades de ordenação e consultas que tornam desnecessárias sua implementação no código da ferramenta.

8. **Importar relatórios de planilhas eletrônicas:** Importar relatórios de planilhas eletrônicas é um requisito que facilita a correção de uma determinada informação

ou conjunto de informação que foram identificadas quando da confecção de matriz de comparação de critérios (Método AHP) Esse item faz parte de um conjunto de requisitos relacionados à utilização do método AHP no processo decisório, que permitiria, à ferramenta, a criação de uma matriz de comparação de critérios de forma gráfica, possibilitando ao usuário do sistema a comparação dos critérios par a par.

9. **Confecção de matriz de comparação de critérios (Método AHP):** Criação de matriz quadrada com os critérios selecionados à análise de risco do contexto estudado. Destina-se ao estabelecimento do Vetor de Eigen, que determina o peso que cada critério terá na análise, como um todo.

10. **Criação de matriz de comparação de ativos por critério (Método AHP):** Esse item também faz parte do conjunto de requisitos necessários à utilização do método AHP. Na verdade, ele é um desdobramento do método e o seu objetivo é o de que a ferramenta também possa criar uma matriz de comparação, utilizando todos os ativos a serem analisados, critério por critério, de forma que, se houvessem dez critérios, haveriam, nesse caso, dez matrizes.

11. **Criação de relatórios por grupo de ativos:** Esse item visa permitir o agrupamento de um determinado tipo de ativo de TI, de forma que a ferramenta possa tratar esse grupo individualmente, transportando para o grupo, o maior índice de determinado atributo, ou a sua média, de acordo com o que for mais pertinente à análise de risco.

12. **Criação de relatórios de análise de risco:** Relatórios servem para exibir informações consolidadas das últimas avaliações de riscos. Esses relatórios podem ser customizados e, antes que sejam gerados, podem ser filtrados para mostrar apenas informações específicas. Uma vez gerados, devem poder ser enviados por e-mail ou exportados em diversos formatos, desde editáveis, como txt, doc, docx, até aqueles somente para leitura, como xml ou pdf. A geração no formato de planilhas eletrônicas foi tratada como um requisito à parte, por conter especificidades que o distingue de um relatório comum.

13. **Instalação em plataforma Windows:** Esse item não se trata de um requisito funcional, mas possui extrema relevância se considerarmos que os ambientes de TI dos diversos órgãos da APF são heterogêneos com relação à plataforma existente. Determinar a usabilidade de uma ferramenta nessa plataforma pode significar a sua utilização ou não.

14. **Instalação em plataforma Linux:** Esse item apresenta a mesma relevância do requisito anterior, guardadas as especificidades de cada plataforma. As distribuições Debian, Suse, Red Hat, Slackware, por exemplo, apesar de serem todas Linux, possuem particularidades quanto a bibliotecas, dll's e applets, que tornam fácil a instalação das ferramentas, ou não.

15. **Possuir rotinas de backup e restauração:** Esse item não é um requisito funcional, mas apresenta relevância extrema, se considerarmos que qualquer ferramenta que manipule uma quantidade significativa de informação necessita ter implementada uma rotina de backup automática e, ainda, uma rotina de recuperação dessas informações.

16. **Integração com o Active Directory (AD):** Esse item visa possibilitar a integração com um serviço de diretório no protocolo LDAP que armazena informações sobre objetos em rede de computadores e disponibiliza essas informações a usuários e administradores dessa rede. O AD é, na verdade, um software da Microsoft utilizado em ambientes Windows.

17. **Integração com o LDAP:** O LDAP ou Lightweight Directory Access Protocol é um protocolo de aplicação aberto, livre de fornecedor e padrão de indústria para acessar e manter serviços de informação de diretório distribuído sobre uma rede. Esse item visa possibilitar a integração com um serviço de diretório nas distribuições Linux que recebem o mesmo nome do protocolo LDAP.

4.5 Estudo de Caso da Ferramenta Modulo Risk Manager

Após extensiva busca e diversas solicitações de informações complementares enviadas aos contatos listados nos sítios, as únicas empresas que responderam aos questionamentos foram a eGestalt Technologies SecureGRC, representante da ferramenta Aegify vMarch2014 e a Modulo Solutions for GRC, representante da ferramenta Módulo Risk Manager. As ferramentas destas empresas encontram-se no mesmo grupo de análise apresentada na revista, quer seja, a gestão de riscos. No entanto, somente a Modulo possui representação no Brasil e, por isso, o estudo passou a se concentrar na utilização da ferramenta Risk Manager como insumo básico para extração de requisitos funcionais e não-funcionais necessários ao cumprimento do terceiro objetivo específico deste trabalho.

No Brasil, a empresa Módulo Security Solutions, que é nacional, fabrica a ferramenta Risk Manager, líder nos segmentos de Segurança da Informação e Gestão de Vulnerabili-

dades em TI, Gestão de Riscos Operacionais, Gestão de Riscos Corporativos, de Centros Integrados de Operações para Gestão por Indicadores, Cidades Inteligentes e Grandes Eventos.

Sem ter uma outra ferramenta disponível no mercado brasileiro para atuar no segmento de gestão de risco e compliance, ela é, no momento, a única alternativa do mercado. A empresa também possui atuação internacional, atuando de forma específica no mercado americano.

Após algumas tentativas de contato com a empresa, o autor desta dissertação conseguiu agendar uma reunião com representantes técnicos da empresa, na qual foi apresentada uma minuta da pesquisa para todos os presentes. A empresa mostrou-se inicialmente interessada em contribuir com a pesquisa, fornecendo todos os subsídios necessários à fase de levantamento de requisitos.

Após essa reunião, a empresa disponibilizou, no mês de dezembro de 2014, um equipamento com a versão instalada da ferramenta e, somente no mês de janeiro de 2015, pôde disponibilizar um técnico da área para que, junto com este autor, realizassem uma prova de conceito (POC) na infraestrutura de rede do DSIC com o objetivo de verificar se a ferramenta poderia ser adaptada para a realização da análise de riscos financeiros sobre os ativos de rede do DSIC.

Nessa POC, foram verificados os módulos de cadastramento da ferramenta. Inicialmente foi visto os módulos de cadastramento de contexto interno, em conformidade a com a norma ISO 31.000. O estabelecimento do contexto é feito estabelecendo-se o perímetro em que foi feita a análise de risco, como pode ser visualizado na figura 4.15.

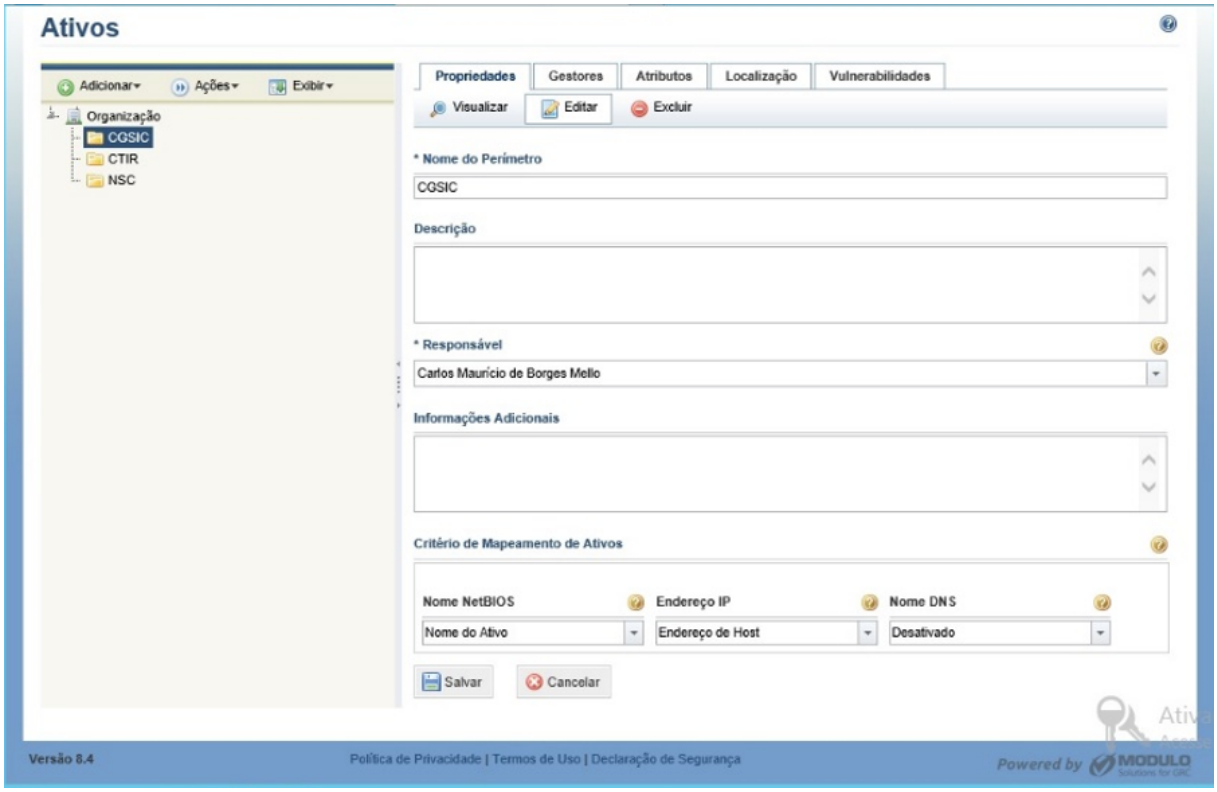

Figura 4.15: Modulo RM – Estabelecendo o contexto [26].

Esses perímetros podem ser de diversos tipos, a ferramenta é bastante flexível nesse ponto. Assim, o perímetro pode representar um rack, uma seção, um departamento ou mesmo um órgão. Uma vez estabelecido, os ativos podem ser cadastrados dentro desses perímetros. A vantagem de agrupar os ativos por perímetros é que podem ser feitos ajustes e análises específicas por perímetro estabelecido.

O sistema permite, ainda, a alocação de gestores para esse perímetro, que podem ser desde uma pessoa até um grupo de pessoas. O perímetro pode ter também seus atributos customizados para que sejam inseridos e armazenados em um conjunto varável de informações específicas.

Adicionalmente ao cadastro do perímetro, a ferramenta permite o cadastro de ativos (Figura 4.16), que podem, inclusive, ser criados por tipo: tecnologia, processo, pessoa e ambiente. É possível a criação de tipos customizados de ativos, o que não é o foco desta pesquisa, pois, no nosso estudo, o ativo do tipo “tecnologia” atende à necessidade do estudo.

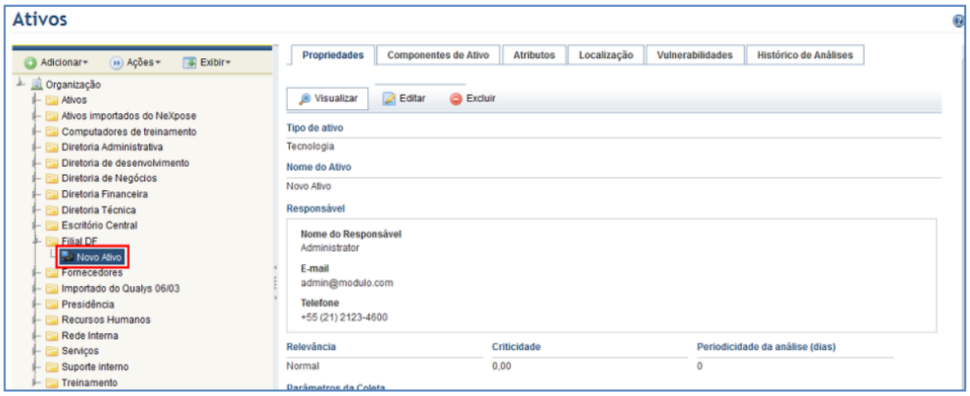

Figura 4.16: Modulo RM – Cadastro de ativos [26].

Ao cadastrar um ativo, é possível a inserção de diversos atributos. Alguns já inerentes ao tipo do ativo, porém, a ferramenta possibilita, ainda, a criação de atributos adicionais que podem ser criados, editados e selecionados para exibição pelo usuário do sistema. Existe uma enorme lista de atributos que podem ser criados para cada objeto padrão e mesmo que ele não esteja nessa lista, pode-se usar o artifício de usar o atributo "Texto" para a inserção customizada de um atributo. Dentro das possibilidades existem Anexos, Data/hora, E-mail, Fórmula, Georreferência, Imagem, Link, Lista de opções, Número, Parágrafo, Relacionamento, Texto e Tópicos. Esses atributos não estão disponíveis para todos os objetos e sua criação é bem flexível, com telas de ajuda muito bem elaboradas e intuitivas. A figura 4.17 apresenta uma tela de criação do atributo "Imagem", na qual podem ser customizados diversos parâmetros inerentes ao atributo ou ativo.

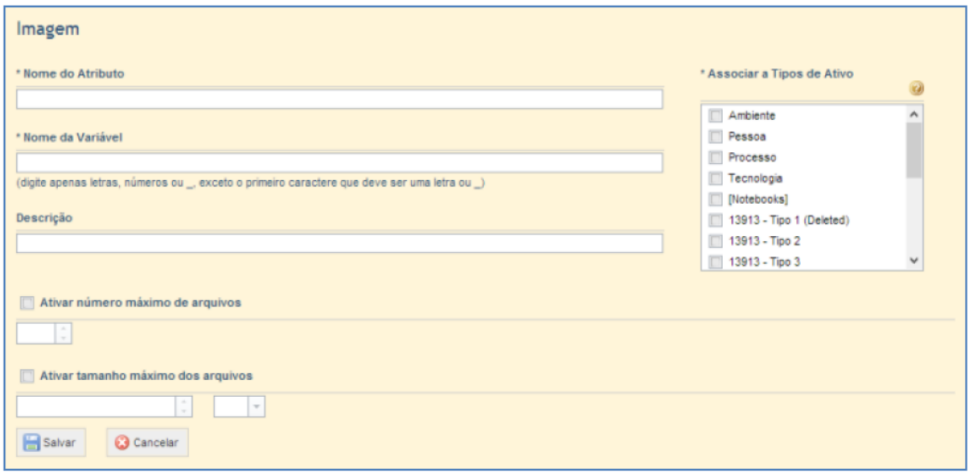

Figura 4.17: Modulo RM – Criando atributos de ativo [26].

A customização do atributo dá a ferramenta uma flexibilidade de ações, pois permite ao analista a criação customizada que pode, em um segundo momento, ser utilizado para outras atividades.
Uma vez que os perímetros e os ativos estejam cadastrados, a ferramenta possibilita consultas ao módulo organização, que podem ser dos tipos ERM, de Riscos, de Compliance e Workflow. As consultas podem ser consolidadas pelos seguintes elementos: agrupamento, ameaça, ativo, componentes de negócio, componentes de ativo, controle, fonte de ameaça, KB e perímetro.
A consulta por agrupamento interessa na pesquisa, pois diversos ativos a serem cadastrados podem ser agrupados por tipo para que a análise de risco em investimentos em TI seja feita por grupos de ativos e não por ativo isoladamente.
A ferramenta permite a exportação de relatórios customizados que podem ser exportados e editados em uma planilha e importados novamente para o sistema. Objetos, ativos ou atributos não podem ser excluídos por essas funcionalidades. Isso é bastante útil porque permite a criação e a edição de uma estrutura organizacional dentro e fora do sistema. A figura 4.18 mostra a tela inicial do módulo de exportação de relatórios.

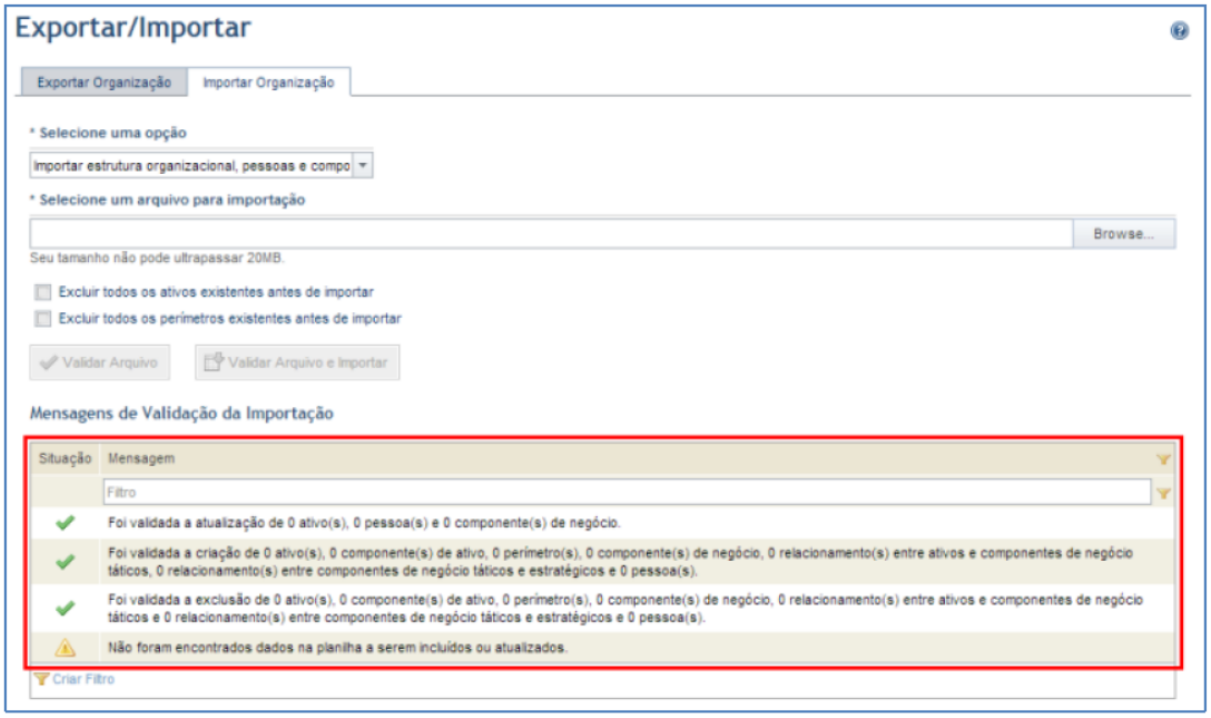

Figura 4.18: Modulo RM – Exportar relatório [26].

Essa funcionalidade é desejável à pesquisa porque permite a visualização integrada de todos os atributos e, devido à possibilidade de importação para o sistema, seria possível

a correção de eventuais distorções ou ajustes ainda na fase de análise.

A ferramenta gera diversos tipos de relatórios, desde genéricos até os específicos de risco. Os genéricos podem ser criados desde o início e permitem a inclusão de consultas específicas de outras seções da ferramenta, como organização, de riscos, de eventos e até mesmo a integração com consultas SQL[4] como fonte de dados. Os relatórios permitem customização para inserção de logos das empresas, capas, seções, gráficos e tabelas.

Os relatórios de risco, apesar de se poder acessá-los através de qualquer usuário que acesse a página da ferramenta, ficará restrito ao nível de acesso que tal usuário tenha. Muitos desses relatórios são resultados de questionários que foram elaborados e respondidos. O processo de tomada de decisão sobre investimentos previsto na ferramenta não faz alusão à tomada de decisão pretendida nesta pesquisa, haja vista, todas as decisões da ferramenta se reportarem a riscos tecnológicos e não riscos financeiros.

A ferramenta da Modulo disponibiliza, para as ações de criação de relatórios, o programa Report Designer. A edição dos relatórios mencionada anteriormente, só pode ser feita através desse aplicativo, que é um programa à parte e deve ser baixado e instalado separadamente. O detalhe desse programa é que ele funciona semelhante a um editor de texto padrão, porém somente abre e edita os relatórios gerados pela ferramenta da Modulo. Abaixo é mostrado a figura 4.19 com o detalhe de edição de um relatório, com a inserção de uma imagem.

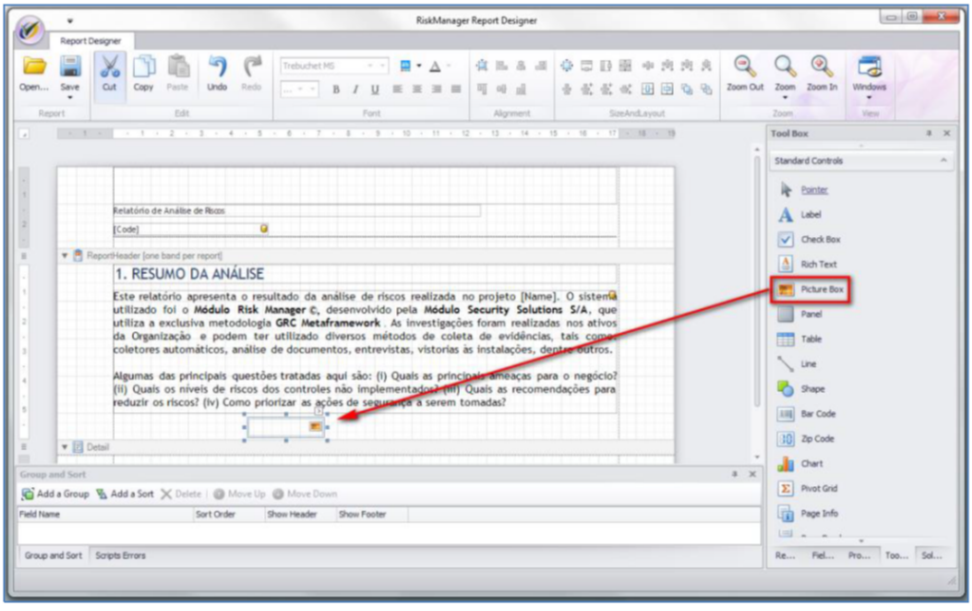

Figura 4.19: Modulo RM – Edição de relatório [26].

[4]Structured Query Language, ou Linguagem de Consulta Estruturada ou SQL, é a linguagem de pesquisa declarativa padrão para banco de dados relacional utilizada pelos principais softwares, como Oracle, Microsoft SQL Server, PostgreSQL, MySQL, entre outros.

Detalhes de características, funcionalidades e “How to” – “Como fazer” ” – do programa podem ser encontrados no manual da ferramenta, disponibilizado pela Modulo.
Após inúmeras reuniões com os técnicos da empresa, foi constatado que, apesar da ferramenta da Módulo Security Solutions, ser muito customizável, mesmo ela não seria capaz de realizar as análises pretendidas, sob o ponto de vista de investimentos, e tanto os técnicos, quanto este pesquisador concluíram que a ferramenta serviria apenas como um repositório de informações dos ativos, sem, contudo, conseguir realizar uma análise e consequente apresentação de escalas de riscos a que os ativos de TI estariam sujeitos.
Assim, concluiu-se que há necessidade da construção de uma ferramenta específica para a área de TI, na qual seja possível levantar prioridades para a tomada de decisão de investimentos em tecnologia da informação.
Tendo isto como premissa final da pesquisa, os itens a seguir, apresentam um plano de definição de software que descreve de forma sequencial, as etapas necessárias à construção de uma nova ferramenta de análise de riscos em investimentos de TI através e, principalmente, do levantamento de seus pretensos requisitos.

4.6 Consolidação dos requisitos elicitados

A partir do estudo desses requisitos, as ferramentas selecionadas anteriormente, foram novamente analisadas em busca da conformidade e o resultado obtido pode ser visualizado na tabela 4.6, constante do Apêndice A, desta pesquisa.

Tabela 4.6: Elicitação de requisitos detalhado por ferramenta (Apêndice A)

Capítulo 5

Análise e Especificação de Requisitos e Critérios para uma Ferramenta que atenda à demanda do contexto

5.1 Especificação da nova ferramenta

A análise de risco de uma infraestrutura de tecnologia de informação proposta para a pesquisa seria uma que, ao invés de ter como ponto focal as vulnerabilidades técnicas, teria como foco os detalhes técnicos pertinentes a uma contratação de bens ou serviços. Assim, fatores como atualizações de drivers de componentes físicos, atualização de licenças de software, ou ainda varreduras para verificação de portas de comunicação, que deveriam estar configuradas de um modo ou de outro, não são requisitos essenciais desta pesquisa. O levantamento dos requisitos de um sistema, software ou framework deve ser listado pela necessidade de se avaliar o grau de prioridade que a atenção a um determinado ativo tenha ou não para ser observado pelo gestor de TI. Essa observação seria objeto de outra análise, agora puramente para investimentos.
A decisão de qual tipo de investimento fazer depende agora de quanto recurso pode ser alocado ao ativo que tem a prioridade de investimento. As ações sobre um ativo variam de acordo com a natureza do ativo. O Guia de Boas Práticas em Contratações de Soluções de TI, expedido pela SLTI do MPOG – indica no art, 4º, da Instrução Normativa IN 04/2014 [8], o seguinte:

> Art. 4º As contratações de que trata esta IN deverão ser precedidas de planejamento, elaborado em harmonia com o Plano Diretor de Tecnologia da Informação – PDTI. § 1º O PDTI deverá estar alinhado à EGTI e ao plano estratégico institucional e aprovado pelo Comitê de Tecnologia da Informação do órgão ou entidade. § 2º Inexistindo o PDTI, o órgão ou entidade deverá proceder à sua elaboração, observando, no que couber, o Guia de Elaboração de PDTI do SISP, acessível no Portal do SISP. § 3º Inexistindo o plano estratégico institucional, sua ausência deverá ser registrada no PDTI e deverá ser utilizado um documento equivalente, como o Plano Plurianual – PPA. (2014)

Assim, após terem sido estabelecidas as prioridades dos ativos de rede, elas devem ser submetidas ao previsto na IN 04 e precedidas de planejamento. e para executar esta fase, é necessário cumprir as seguintes etapas:

- instituição da equipe de planejamento da contratação;
- estudo técnico preliminar da contratação;
- análise de riscos; e
- elaboração do termo de referência ou projeto básico.

A etapa de estudo técnico preliminar da contratação deve ser realizada pelos integrantes Técnico e Requisitante, e é composta pela definição e especificação das necessidades do negócio e tecnológicas e do levantamento de requisitos necessários para a correta escolha da solução de tecnologia da informação a ser contratada ou adquirida.
Tendo como premissa a necessidade de encontrar uma ferramenta de análise de risco para a tomada de decisão de investimentos na área de tecnologia da informação (ativos de rede), os requisitos necessários a uma ferramenta seriam os estabelecidos e, contidos no plano de definição de software.

5.1.1 Objetivos

A especificação dos requisitos deve conter o conjunto de ações que devem ser atendidas pelo software de análise de risco com ênfase em investimentos de tecnologia da informação, de forma que satisfaça as necessidades do gestor de TI do órgão, assim como estabelecer o escopo do produto a ser futuramente desenvolvido.
O público-alvo desse conjunto de requisitos são os clientes (gestores de TI e desenvolvedores do provável software).

5.1.2 Escopo do software

O produto não possui um nome determinado, mas seria um software composto por um componente único, cuja finalidade destina-se ao apoio aos gestores de TI na análise de risco de ativos de rede com ênfase em investimentos.

5.1.3 Limites do software

Dentre as limitações do software, podem-se destacar as seguintes:

- o software não realizará análise de riscos voltadas a vulnerabilidades dos ativos;
- o software não realizará inventário de ativos de rede automaticamente através de agentes ou plug-ins;
- o software não possuirá um módulo de ajuda online. No entanto, contará com um manual de uso;
- o software não realizará back-up das suas bases de dados automaticamente. As rotinas de back-up deverão ser realizadas pela administração de dados dos órgãos.
- o software não realizará indicação sobre qual tipo de investimento deve ser realizado no ativo. Ele apenas indicará qual o ativo que deve ser priorizado para investimento.

Convém destacar que, no processo de contratação, de acordo com a IN 04/2014, na etapa de estudo técnico preliminar da contratação é que será decidido qual a linha de ação a ser tomada com relação ao ativo.

5.1.4 Benefícios esperados do Software

O software irá proporcionar uma lista de prioridades dos ativos a serem observados, sob a óptica de investimento. Seus cálculos possibilitarão ao Gestor se basear em critérios matemáticos bem definidos e alinhados com suas perspectivas financeiras.
É importante destacar que a ferramenta utiliza o método de análise hierárquica (AHP) para mensurar os valores indicados para cada ativo. Assim, fica evidente que o software agregará qualidade no processo decisório, se comparado com processos puramente empíricos utilizados no cotidiano da maioria dos órgãos públicos da APF.
Os itens, que se seguem nesse capítulo, apresentam os requisitos e critérios que atendam à demanda do contexto. Todos os requisitos e critérios estão inseridos no Plano de Definição de Software, detalhado adiante.

5.2 Plano de definição de software

Este Plano é um documento que tem como finalidade elicitar os requisitos necessários para o desenvolvimento de uma ferramenta para gestão de risco de ativos em TI, a partir do entendimento do processo de negócio existente, que servirá de base para a identificação dos seus problemas, e a partir deste ponto, mapear um novo fluxo, descrevendo os elementos básicos para construção de uma solução de software.
A metodologia utilizada procura ter "como base a qualidade, se alicerça em processo, dispõe de métodos que fornecem a técnica de como fazer e utiliza apoio automatizado de

ferramentas"[29].
Os mapeamentos de processos foram feitos utilizando o BPMN – Business Process Modeling Notation, através da ferramenta Bizagi Process Modeler.
Os requisitos foram levantados, com base no negócio do DSIC, especificamente, em seu processo de contratação de bens e serviços de TI, utilizando o método iRON (integração de Requisitos Orientados a Negócio) e com o apoio da ferramenta iRON Explorer [13].

5.2.1 Análise institucional

1. A organização
   O DSIC é um dos órgãos que compõe o GSI/PR. Sua estrutura organizacional, conforme organograma ilustrado na Figura a seguir, contempla as seguintes Coordenações:

   - Coordenação-Geral de Gestão de Segurança da Informação e Comunicações (CGGSIC);
   - Coordenação-Geral de Tratamento de Incidentes de Redes (CGTIR);
   - Coordenação-Geral do Sistema de Segurança e Credenciamento (CGSSC).
   - Além destas Coordenações, o DSIC conta com 03 (três) setores de apoio: a Assessoria, o Gabinete e o Grupo de Apoio Técnico (GAT).

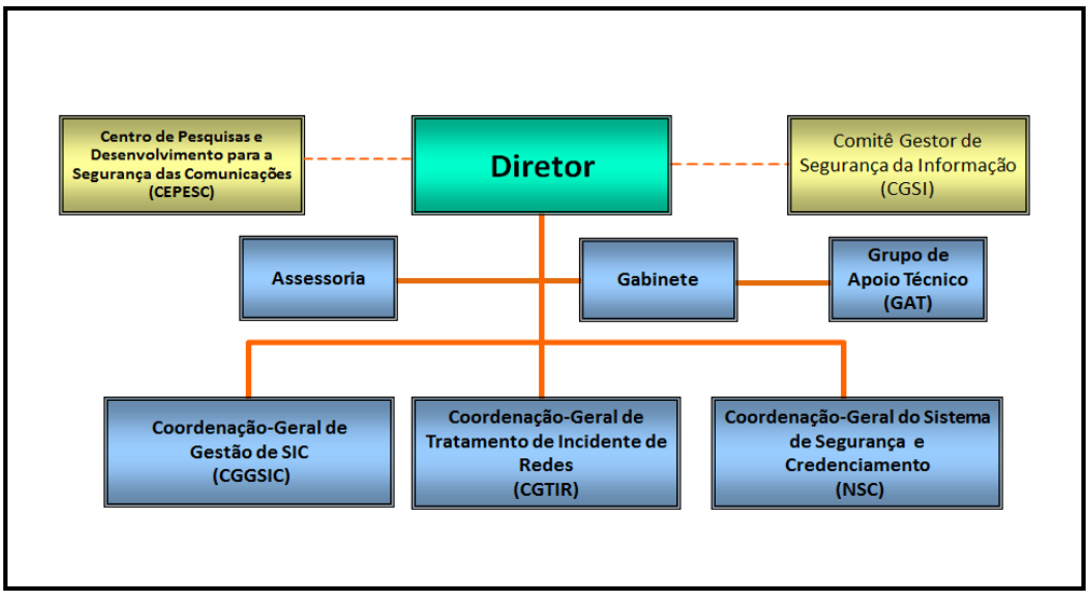

Figura 5.1: Organograma Funcional do DSIC .

2. O negócio

   O GAT é o responsável pela governança de tecnologia da informação do DSIC. Nesse processo de gestão, são realizadas as seguintes atividades:

   - Levantamento de demandas de TI
   - Levantamento de oportunidades de TI
   - Gestão do orçamento de TI
   - Gestão de riscos de TI
   - Planejamento de contratação de TI

   Dentre essas atividades, pode-se destacar o controle do orçamento de TI como sendo o prioritário, pois não é raro observar escassez de recursos para a área de TI nas diversas esferas do Governo Federal.
   A contratação de bens e serviços da administração pública federal é regulada pela IN nº 04/2014, editada pela SLTI do MPOG, que reúne um conjunto de políticas, diretrizes e normas relativas a todo o processo de aquisição de bens e serviços, bem como o processo de gestão dos recursos de TI. O mais relevante dessa IN é o fato de que ela criou uma cultura buscando o alinhamento estratégico da área de TI, não só com a área finalística, mas com as demais áreas da organização.
   Com a implantação da IN 04 as contratações de TI passaram a ser vinculadas aos planejamentos estratégicos institucionais, haja vista as organizações serem cada vez mais dependentes de soluções de TI para o alcance de seus objetivos.
   Esse processo do GAT pode, então, ser sintetizado pelas seguintes ações:

   - Levantamento das necessidades de contratação de TI, de acordo com o Plano de Metas e Ações publicados no Plano Diretor de Tecnologia da Informação (PDTI);
   - Levantamento do orçamento disponível para a área de TI;
   - Estudo preliminar do orçamento;
   - Solicitação de propostas às empresas fornecedoras de solução de TI;
   - Consolidação e análise das propostas orçamentárias;
   - Análise de Viabilidade Orçamentária.

   Nesse ponto, o processo pode ter duas situações: A primeira, é a de que o recurso orçamentário é suficiente para atender a todas as demandas previstas no PDTI e, nesse caso, o gestor inicia a execução orçamentária, com os processos de contratações preconizados pela IN 04. A segunda opção, é a de que o recurso orçamentário não

é suficiente para atender a todas as demandas previstas no PDTI. Nesse segundo cenário, o Gestor executa as seguintes ações:

- Consolidação de um relatório de viabilidade orçamentária;
- Envio desse relatório à autoridade competente para determinação de prioridades;
- Recebimento das prioridades;
- Execução das contratações até o limite orçamentário.

A partir desse ponto, ambas as situações convergem para o mesmo desfecho, a saber a execução das contratações que são feitas mediante calendário de execução, para o caso do orçamento ser suficiente para todas as demandas, ou mediante a lista de prioridades estabelecida pela autoridade competente.

5.2.2 Mapeamento do processo de contratação de TI no DSIC (Fluxo atual)

Nesta etapa foi mapeado o processo de contratação de TI do DSIC, como ele é estruturado no momento. Este mapeamento é conhecido como Modelo "As Is", pois retrata o processo atual.
Ele está simbolicamente apresentado na figura 5.2, a seguir, porém, pode ser melhor visualizado em tamanho ampliado, no Apêndice B.

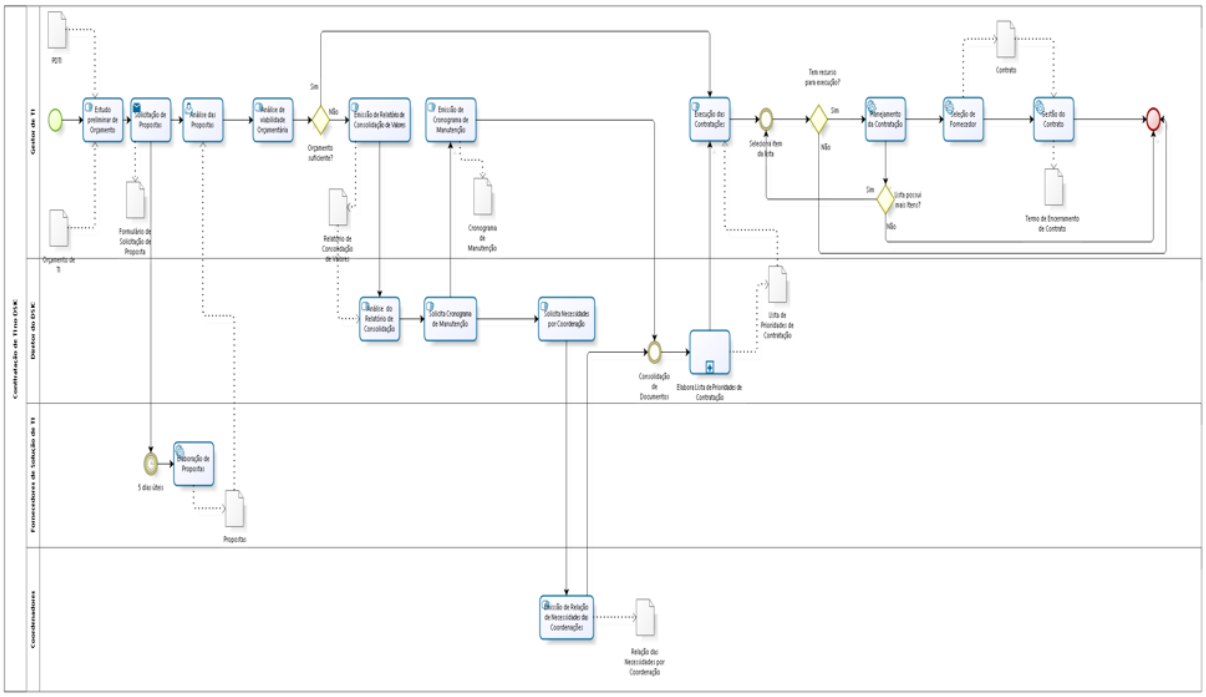

Figura 5.2: Mapeamento do Processo de Contratação de TI (DSIC) "As Is".

5.2.3 Análise Funcional

1. Área envolvida:
   A área central envolvida pelo sistema, a ser desenvolvido, será o próprio GAT que é a Unidade que detém a gestão de TI do DSIC, onde o foco será o processo decisório sobre quais equipamentos devem ser priorizados no eventual contingenciamento de recursos orçamentários.

2. Descrição do processo decisório:
   O GAT realiza as atividades de gestão de TI do DSIC, com base em dois documentos fundamentais, que são o PDTI e a Dotação Orçamentária do DSIC para o ano-base. Inicialmente é feito um levantamento de preços de todas as necessidades de TI listadas no PDTI. Esse levantamento é feito mediante a solicitação formal às empresas prestadoras de serviços ou soluções de TI, de proposta/orçamento de cada ativo listado no PDTI.
   Essas propostas/orçamentos são então, analisados, catalogados e acumulados no Plano geral, onde é feita uma totalização preliminar que demonstra qual o orçamento necessário para a execução de 100% do Plano de Metas do Departamento, elencado no PDTI.
   Neste momento o GAT realiza a análise financeira do Plano de Metas e, caso verifi-

que que o orçamento disponibilizado ao DSIC é suficiente para sua execução, inicia os processos de contratação executando cada item do Plano, à medida em que as demandas vão se apresentando, quer seja por tempo, quer seja por necessidade de manutenção.
Caso a análise financeira indique que não há recursos financeiros suficientes para a execução de todo o Plano de Metas, um relatório consolidado dessa análise é produzido e encaminhado ao Sr. Diretor do DSIC para que este, indique as prioridades com que as contratações devem ser realizadas, até o fim do recurso orçamentário.
Nesse processo de indicação de prioridades, o Sr. Diretor solicita duas informações complementares:

- Primeira: Ao GAT – Um cronograma de necessidade de execução das contratações de TI. Para ilustrar essa solicitação, pode ser citado como exemplo, informações que determinam a ordem cronológica das necessidades de TI, tipo listar os ativos de TI por data de término de garantia, ou renovação de contrato; e
- Segunda: Às Coordenações – Um rol de prioridades com que estes equipamentos devem ser manutenidos, de acordo com as necessidades de cada Coordenação.

Essas demandas auxiliam o Sr. Diretor a decidir as prioridades com que serão executadas as contratações. Após essa definição ter sido divulgada ao GAT, esse setor inicia a execução orçamentária, e essa execução será realizada ciclicamente cumprindo uma sequência de eventos que pode ser visualizada no recorte do mapeamento do processo, abaixo:

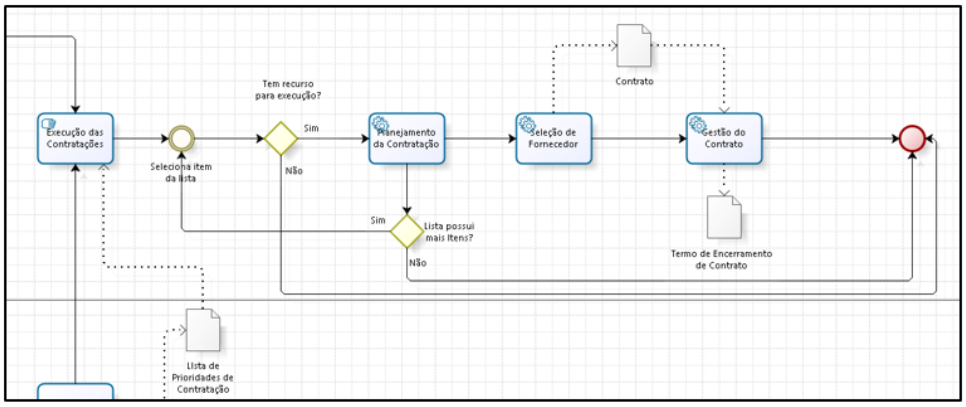

Figura 5.3: Detalhe: Execução orçamentária - Fluxograma .

Nesse recorte, pode ser visto que cada item da lista é selecionado, e então é verificada a disponibilidade de recurso para sua execução. Se houver tal disponibilidade, o processo caminha para o planejamento da contratação, e ato contínuo, um novo item da lista é selecionado.

O processo termina quando não houver mais itens na lista, ou quando não houver mais recurso orçamentário para sua execução.

3. Identificação dos problemas:

   - **Falta de critério de escolha:**

Tabela 5.1: Problema no processo atual: Falta de critério de escolha

Nome	**Justificativas**
O problema de:	Falta de critério para a elaboração da lista de prioridades.
Afeta:	A execução do plano orçamentário.
Cujo impacto é:	Uso do recurso de forma não otimizada.
Benefícios de uma solução seriam:	Uso racional do recurso orçamentário, propiciando um melhor aproveitamento em prol do DSIC.

   - **Montagem da lista de prioridade baseada em linha temporal:**

Tabela 5.2: Problema no processo atual: Montagem da lista de prioridade baseada em linha temporal

Nome	**Justificativas**
O problema de:	Montagem da lista de prioridades baseada em uma linha temporal.
Afeta:	A execução orçamentária face à necessidade de alinhamento estratégico da TI com o planejamento estratégico institucional.
Cujo impacto é:	Solução de continuidade nos serviços mais relevantes para o objetivo do DSIC.
Benefícios de uma solução seriam:	Uso racional do recurso orçamentário, propiciando um melhor aproveitamento em prol do DSIC.

- **Montagem da lista de prioridades baseada na demanda das Coordenações:**

Tabela 5.3: Problema no processo atual: Montagem da lista de prioridades baseada na demanda das Coordenações

Nome	Justificativas
O problema de:	Montagem da lista de prioridades baseada na demanda das Coordenações.
Afeta:	A execução orçamentária face à necessidade de alinhamento estratégico da TI com o planejamento estratégico institucional.
Cujo impacto é:	Solução de continuidade nos serviços gerais que contribuem para o alcance do objetivo do DSIC.
Benefícios de uma solução seriam:	Uso racional do recurso orçamentário, propiciando um melhor aproveitamento em prol do DSIC.

5.2.4 Proposta de Solução

1. : **Objetivo geral:**
   Desenvolver um software de análise de risco para a tomada de decisão de investimentos financeiros na área de tecnologia da informação – ativos de rede, permitindo análises de critérios específicos, sob o ponto de vista financeiro, que direcionem os esforços de execução orçamentária para a elaboração de uma lista de prioridades otimizada pela combinação de múltiplos critérios.

2. **Objetivos específicos:**

   - Levantamento dos ativos de TI a serem analisados

Tabela 5.4: Objetivos da solução: Levantamento dos ativos de TI a serem analisados

Nome	Justificativas
Objetivos específicos:	Realizar o levantamento dos ativos de TI que serão objetos da análise de riscos para investimentos em TI.
Prioridade:	Alta.
Proposta de solução:	Desenvolvimento de um sistema que permita o cadastro de ativos de TI, com diversos atributos.
Funcionalidades:	Cadastramento do ativo de TI – Cadastramento de atributos de ativos de TI.

- Levantamento dos fornecedores de ativos de TI

Tabela 5.5: Objetivos da solução: Levantamento dos fornecedores de ativos de TI

Nome	**Justificativas**
Objetivos específicos:	Realizar o levantamento dos fornecedores de ativos de TI que serão consultados pelo sistema para levantamento de critérios dos ativos de TI.
Prioridade:	Baixa.
Proposta de solução:	Desenvolvimento de um sistema que permita o cadastro dos fornecedores de ativos de TI, com diversos atributos.
Funcionalidades:	Cadastramento de fornecedores de ativo de TI – Emissão de mensagens eletrônicas para solicitar dados de ativos de TI.

- Elaboração dos critérios de análise de riscos

Tabela 5.6: Objetivos da solução: Elaboração dos critérios de análise de riscos

Nome	**Justificativas**
Objetivos específicos:	Realizar o cadastro dos critérios de análise de risco.
Prioridade:	Alta.
Proposta de solução:	Automação no processo de composição dos critérios utilizados na análise de risco.
Funcionalidades:	Definição de critérios de análise de risco – Criação dos critérios.

- Cálculo do peso dos critérios de análise de risco

Tabela 5.7: Objetivos da solução: Cálculo do peso dos critérios de análise de risco

Nome	**Justificativas**
Objetivos específicos:	Calcular o peso que cada critério terá sobre o resultado final do sistema.
Prioridade:	Alta.
Proposta de solução:	Aplicação de análises técnicas, par a par, sobre todos os critérios de análise de risco a partir de uma matriz quadrada de forma a calcular, com precisão, o grau de relevância que cada critério possui no processo de análise de risco, como um todo.
Funcionalidades:	Geração de uma matriz quadrada para inserção da análise par a par dos critérios e, geração do cálculo do peso que cada critério possui, no processo, como um todo.

- Cálculo do peso dos ativos por critério na análise de risco

Tabela 5.8: Objetivos da solução: Cálculo do peso dos ativos por critério na análise de risco

Nome	**Justificativas**
Objetivos específicos:	Calcular o peso que cada ativo possui quando analisado exclusivamente por um dos critérios na análise de risco.
Prioridade:	Alta.
Proposta de solução:	Aplicação de análises técnicas, par a par, sobre todos os ativos de TI, levando-se em consideração um único critério da análise de risco a partir de uma matriz quadrada de forma a calcular, com precisão, o grau de relevância que cada ativo de TI possui no processo de análise de risco, quando considerado um único critério. Esse cálculo se repetirá tantas vezes quantas forem os critérios cadastrados.
Funcionalidades:	Geração de uma matriz quadrada para inserção da análise par a par dos ativos de TI, tomando como referência o critério escolhido – Geração do cálculo do peso que cada ativo de TI possui, no processo, como um todo.

- Consolidação da análise de risco dos ativos de TI

Tabela 5.9: Objetivos da solução: Consolidação da análise de risco dos ativos de TI

Nome	Justificativas
Objetivos específicos:	Combinar o peso que cada ativo possui isoladamente por critério, num único resultado ponderado por análise de multicritério.
Prioridade:	Alta.
Proposta de solução:	Aplicação da Análise de Multicritério para consolidação dos múltiplos pesos que cada ativo tem quando comparado critério por critério. Esse cálculo consolida os ativos por prioridade de execução orçamentária, informando qual ativo possui o maior risco sob o ponto de vista orçamentário.
Funcionalidades:	Geração de uma lista dos ativos de TI priorizados por risco de investimento – Geração de detalhamento, por ativo de TI, dos resultados obtidos em cada critério analisado.

5.2.5 Descrição do Processo Proposto

A gestão de TI no DSIC é feita pelo GAT. Porém, não há uma definição sobre o processo decisório, ou seja, não há um setor ou responsável claramente definido para o estabelecimento de prioridades para execução orçamentária, caso haja o problema de não se ter recurso orçamentário suficiente para a execução do plano de manutenção orgânica dos ativos de TI do Departamento.
Esse procedimento é feito empiricamente pelo Diretor do Departamento, que se baseia somente em dois parâmetros para tal atividade:

- Cronograma de vencimento das garantias e/ou contratos de manutenção em vigor; e
- Necessidade pontual informada pelos Coordenadores das áreas com atividades-fim.

Assim, não raro, as prioridades preestabelecidas são modificadas ao longo do ano de exercício fiscal, por demandas pontuais apresentadas, inopinadamente, por um ou outro coordenador, quando assim surgem.
O sistema proposto visa consolidar um grupo de critérios técnicos, sob o ponto de vista orçamentário, além de um critério técnico, Fator de Risco, para apreciação do ativo de TI frente às necessidades de se cumprir os objetivos da organização.
O sistema prevê o cadastro de alguns tipos de usuários para que estes possam lidar

com diversas fases do processo de análise de riscos. Inicialmente, foram visualizados os seguintes tipos de usuários do sistema:

- **Administrador:**
  A função Administrador do Sistema é uma função predefinida que inclui tarefas úteis para o administrador do sistema, tendo responsabilidade completa pelos seus parâmetros configuráveis, mas não necessariamente pela manutenção do conteúdo das informações.

- **Gestor:**
  A função Gestor é uma função predefinida que inclui as tarefas mais importantes do sistema. Ele tem a responsabilidade de realizar o cadastro de ativos de TI, dos fornecedores, além de incluir as análises de critérios e de ativos de TI por critérios. É o responsável direto pela manutenção dos conteúdos publicados no sistema, bem como de emitir os relatórios disponibilizados.

- **Convidado:**
  A função Convidado é uma função predefinida do sistema que permite ao usuário, responder alguns questionários previamente criados, de forma que suas respostas sejam automaticamente inseridas no sistema. Esse usuário ganha acesso ao sistema através do envio de um link para acesso externo, onde terá permissão de edição apenas no conteúdo disponibilizado, sem que tenha acesso direto ao sistema.

O sistema funciona basicamente no processo de definir os ativos de TI por prioridade de investimento.
Para realização dessa atividade, o sistema opera da seguinte forma: Uma vez definido que não há orçamento suficiente para a execução do plano de manutenção orgânica dos ativos de TI.
Os ativos de TI devem então, serem cadastrados no sistema e alguns parâmetros desses ativos devem ser obrigatoriamente registrados no sistema. Cada ativo deve ser identificado por um código único, descrição, fabricante, preço unitário, preço de manutenção "per call", preço anual do contrato, tempo de vida útil, probabilidade, severidade, relevância, taxa de uso, grupo e status do ativo.
Esses ativos de TI devem ser agrupados, pois um mesmo conjunto de ativos pode ter parâmetros diferenciados, como probabilidade, severidade e relevância, que juntos compõem um dos critérios, o fator de risco. O sistema deve considerar o maior deles, pois quando executa a análise de riscos, ele o faz para os grupos de ativos de TI e não para um ativo, isoladamente.

5.2.6 Critérios da análise de riscos

Os critérios para a análise de risco em investimentos de TI visam, de uma forma geral, observar detalhes que possam mensurar as diversidades financeiras a que os ativos de TI estão sujeitos. Neste item, foram elencados seis critérios que não esgotam as possibilidades de influência, positiva ou negativa, numa eventual análise de riscos a que estes ativos estão sujeitos.

Cada critério é composto por dois ou mais atributos de um ativo de TI e, nessa proposta de sistema, espera-se que esses critérios sejam cadastrados, editados e até mesmo excluídos, se necessário.

Os critérios idealizados nessa fase do projeto foram os seguintes:

1. Preço do atendimento per call

   O atendimento per call, ou "por chamado", envolve um conceito de atendimento comumente utilizado no mercado de TI. Trata-se de uma solicitação de serviço realizada sem que exista, necessariamente, uma relação contratual prévia entre o cliente e o fornecedor do serviço, ou seja, é um atendimento pontual, não previsto, no qual o cliente, necessitando de determinado serviço para seu ativo de TI, contata o fornecedor para que ele emita um orçamento e, se autorizado, o fornecedor realiza o serviço mediante acerto financeiro entre as partes.

   Esse critério é calculado tomando-se por base o valor do contrato do ativo de TI individualizado e pelo valor de um atendimento per call do ativo de TI em questão. O valor do contrato do ativo de TI individualizado significa que, se por ventura houver um contrato único para a manutenção de um conjunto de ativos, esse valor seria o valor do contrato dividido pelo número de ativos que o contrato abrange.

   Esse critério será tanto mais importante para a análise de riscos, quanto for maior o percentual que o preço do atendimento per call representar em relação ao valor contrato do ativo de TI individualizado.

   Isso significa que se esse preço for muito alto, o peso desse critério será alto, também, o que o faz ser diretamente proporcional à análise de riscos, como um todo.

   Para realizar o cálculo e, assim obter a porcentagem do preço de atendimento per call, foi estabelecida a fórmula que pode ser visualizada na figura 5.x:

$$Porcentagem\ do\ Preço\ "Per\ call" = \frac{\text{Preço do atendimento "Per call"}}{\text{Valor do contrato individualizado}}$$

Figura 5.4: Fórmula de cálculo do critério preço atendimento per call.

A porcentagem obtida será considerada diretamente proporcional à análise de riscos, pois quanto maior o percentual obtido, maior será o peso do critério na análise. Isto se deve ao fato de que se um ativo possui um preço per call muito próximo do valor do contrato individualizado, significa dizer que sob o ponto de vista financeiro, a manutenção desse contrato passa a ser mais conveniente para a administração pública.

A fim de criar um indicador para graduar esse critério, e assim poder realizar as etapas seguintes da análise de riscos proposta, foi utilizada a Tabela de Saati [33], que gradua as comparações em escalas de 1, 3, 5, 7 e 9 e, utiliza ainda os valores 2, 4, 6 e 8 como valores intermediários para pequenos ajustes.

Dessa forma, o critério teria seus respectivos indicadores estabelecidos de acordo com a tabela 5.10:

Tabela 5.10: Indicadores do critério: preço atendimento per call

Critério: Porcentagem do Preço Per call	**Valor**
Acima de 90%	9
Acima de 80% até 90%	8
Acima de 70% até 80%	7
Acima de 60% até 70%	6
Acima de 50% até 60%	5
Acima de 40% até 50%	4
Acima de 30% até 40%	3
Acima de 20% até 30%	2
Até 20%	1

2. Preço anual do contrato

   O preço anual do contrato reflete o custo total de uma determinada solução de TI para cada período de 12 meses. Trata-se de um dos critérios principais em decisões de investimento, uma vez que vai impactar diretamente na disponibilidade orçamentária do órgão a cada exercício financeiro.

   Para a composição desse critério, a pesquisa destacou a porcentagem que o preço anual do contrato teria sobre o valor total do orçamento disponibilizado para o órgão no que concerne a gestão de TI. O impacto desse percentual sobre o orçamento, como um todo, pode, de certa forma tornar a gestão de TI inviável, pois se um único contrato consumir um percentual elevado do orçamento, pouco ou nenhum recurso sobrará para a gestão dos demais ativos de TI.

   Esse critério foi concebido para ser estimado através do percentual que o valor anual do contrato representa do orçamento do ano em exercício e, dessa forma, o seu cálculo deve ser realizado, conforme ilustrado na figura 5.5, a seguir.

$$Porcentagem\ do\ Preço\ anual\ do\ contrato = \frac{Preço\ anual\ do\ contrato}{Valor\ do\ orçamento\ do\ ano\ em\ curso}$$

Figura 5.5: Fórmula de cálculo do critério preço anual do contrato .

A porcentagem obtida será considerada inversamente proporcional à análise de riscos, pois quanto maior o percentual obtido, menor será o peso do critério na análise. Isto se deve ao fato de que se um ativo possui um contrato anual cujo valor seja muito próximo do valor total do orçamento disponibilizado ao órgão, significa dizer que sob o ponto de vista financeiro, a manutenção desse contrato passa a ser menos interessante para a administração pública, pois ao celebrar esse contrato todo ou quase todo o recurso disponibilizado seria utilizado e, nesse caso, não haveria mais recurso disponível para a gestão de TI como um todo, reduzindo significativamente, a possibilidade de ajustes de necessidades ou prioridades na gestão dos ativos do órgão.

A fim de criar um indicador para graduar esse critério, e assim poder realizar as etapas seguintes da análise de riscos proposta, foi utilizada a Tabela de Saati [33], que gradua as comparações em escalas de 1, 3, 5, 7 e 9 e, utiliza ainda os valores 2, 4, 6 e 8 como valores intermediários para pequenos ajustes.

Dessa forma, o critério teria seus respectivos indicadores estabelecidos de acordo com a tabela 5.11:

Tabela 5.11: Indicadores do Critério: Preço anual do contrato

Critério: Porcentagem do Preço anual do contrato	**Valor**
Até de 20%	9
Acima de 20% até 30%	8
Acima de 30% até 40%	7
Acima de 40% até 50%	6
Acima de 50% até 60%	5
Acima de 60% até 70%	4
Acima de 70% até 80%	3
Acima de 80% até 90%	2
Acima 90%	1

3. Preço global do produto

   O preço global do produto trata-se da soma dos preços unitários de um determinado grupo de ativos de TI, que para a análise de riscos é tratado como um único elemento. Em geral, quando um contrato de manutenção é firmado, ele é feito para

um determinado grupos de ativos e, não isoladamente, item por item. Assim, esse critério tem estreita relação ao valor que esse ativo, ou grupo de ativos tem, em relação ao patrimônio de TI do órgão.
Esse critério é calculado através do percentual que o Preço global do produto representa sobre o valor total do patrimônio de TI do órgão e, dessa forma, o seu cálculo deve ser realizado, conforme ilustrado na figura 5.6, a seguir.

$$Porcentagem\ do\ Preço\ global\ do\ produto = \frac{\text{Preço global do produto}}{\text{Valor do patrimônio de TI}}$$

Figura 5.6: Fórmula de preço global do produto .

O resultado desse cálculo apresentará o percentual que esse ativo, ou grupo de ativo representa sobre todo o patrimônio calculado e, para fins da análise de riscos proposta, esse valor será considerado diretamente proporcional à atividade, pois, quanto maior o percentual obtido, maior será o peso do critério na análise de riscos. Essa suposição baseia-se no fato de que se um determinado ativo, ou grupo de ativos tem um alto percentual do patrimônio, como um todo, significa dizer que deixa-lo sem proteção de um contrato, por exemplo, representaria em um grande risco para o patrimônio do órgão e, por isso o estabelecimento de um processo de proteção sobre esse ativo seria mais atrativo, pois a administração pública estaria, de certa forma, protegendo seu patrimônio.
A fim de criar um indicador para graduar esse critério, e assim poder realizar as etapas seguintes da análise de riscos proposta, foi utilizada a Tabela de Saati [33], que gradua as comparações em escalas de 1, 3, 5, 7 e 9 e, utiliza ainda os valores 2, 4, 6 e 8 como valores intermediários para pequenos ajustes.
Dessa forma, o critério teria seus respectivos indicadores estabelecidos de acordo com a tabela 5.12:

Tabela 5.12: Indicadores do critério: preço global do produto

Critério: Porcentagem do Preço global do procuto	**Valor**
Acima de 90%	9
Acima de 80% até 90%	8
Acima de 70% até 80%	7
Acima de 60% até 70%	6
Acima de 50% até 60%	5
Acima de 40% até 50%	4
Acima de 30% até 40%	3
Acima de 20% até 30%	2
Até 20%	1

4. Tempo de vida útil

   O tempo de vida útil de um ativo "é o período durante o qual a entidade espera utilizar o ativo ou número de unidade de produção ou de unidades semelhantes que a entidade espera obter pela utilização do ativo" [7]. Em outras palavras, trata-se de uma medida estimada do prazo no qual aquele ativo será útil para a finalidade a que se propõe.

   Ativos próximos à obsolescência tendem a apresentar altos custos de manutenção e baixa performance quando comparados a modelos com lançamento mais recente e, de forma geral, tendem a ser substituídos ou descartados. Assim, a vida útil estimada (total e restante) para determinado ativo é um fator importante a ser considerado em uma decisão de investimento.

   De acordo com a Secretaria do Tesouro Nacional (STN) [7] ocorre depreciação sobre os bens materiais, e para subsidiar esse entendimento define-se depreciação como sendo a redução do valor dos bens pelo desgaste ou perda de utilidade por uso, ação da natureza ou obsolescência.

   Analogamente, para bens intangíveis, como softwares, ocorre a amortização que pode ser definido como sendo a redução do valor aplicado na aquisição de direitos de propriedade e quaisquer outros, inclusive ativos intangíveis, com existência ou exercício de duração limitada, ou cujo objeto sejam bens de utilização por prazo legal ou contratualmente limitado [7].

   Assim, esse critério é montado a partir da depreciação ou amortização do ativo de TI e, seu cálculo deve ser identificado individualmente, item a item, e constantemente atualizado conforme preconizado pela própria STN. Esse cálculo é realizado, principalmente, como resultado de uma avaliação técnica que possa definir o tempo de vida útil pelo qual o bem ainda poderá gerar benefícios para a organização; e o restante do tempo de vida útil do bem, levando em consideração a primeira insta-

lação desse ativo de TI.
Assim, para o estabelecimento dos indicadores desse critério, é necessário o cálculo do tempo de vida útil remanescente do ativo de TI e, esse cálculo é expresso em valores percentuais e deve ser calculado da seguinte forma:

$$Porcentagem\ do\ Tempo\ de\ vida\ útil\ remanescente = 1{,}00 - \frac{Tempo\ de\ uso}{Tempo\ de\ Vida\ útil}$$

Figura 5.7: Fórmula de Tempo de vida útil .

O resultado desse cálculo apresentará o percentual que esse ativo tem de tempo de vida remanescente, obedecidos os critérios de depreciação estabelecidos pela STN para toda a APF.
Para fins da análise de riscos proposta, esse valor será considerado inversamente proporcional à atividade, pois, quanto maior o percentual obtido, menor será o peso do critério na análise de riscos. Essa suposição baseia-se no fato de que se um determinado ativo possui um tempo de vida útil elevado, menor será a necessidade de colocá-lo sob a proteção de um contrato, pois a probabilidade de ocorrer uma pane ou algum evento ou mesmo um incidente que venha a degradar a performance do ativo é mínima. Analogamente a esse raciocínio, pode-se inferir que a situação inversa representa um alto fator de risco, pois essa alta porcentagem indicaria que o ativo de TI, poderia se enquadrar em um ou mais dos seguintes fatores:

- Colapso por desgaste físico, pelo uso ou não;
- Geração de benefícios futuros;
- Limites legais e contratuais sobre o uso
- Exploração do ativo;
- Obsolescência tecnológica

A fim de criar um indicador para graduar esse critério, e assim poder realizar as etapas seguintes da análise de riscos proposta, foi utilizada a Tabela de Saati [33], que gradua as comparações em escalas de 1, 3, 5, 7 e 9 e, utiliza ainda os valores 2, 4, 6 e 8 como valores intermediários para pequenos ajustes.
Dessa forma, o critério teria seus respectivos indicadores estabelecidos de acordo com a tabela 5.13:

Tabela 5.13: Indicadores do Critério: Tempo de vida útil

Critério: Tempo de vida útil	**Valor**
Até de 20%	9
Acima de 20% até 30%	8
Acima de 30% até 40%	7
Acima de 40% até 50%	6
Acima de 50% até 60%	5
Acima de 60% até 70%	4
Acima de 70% até 80%	3
Acima de 80% até 90%	2
Acima 90% (ou indefinido)	1

5. Fator de risco operacional

   O fator de risco operacional refere-se à relevância do ativo, sob o ponto de vista dos serviços que ele suporta, associados à sua probabilidade de uma eventual falha e, ainda, à severidade que essa falha pode representar à organização. Este critério está, portanto, associado ao cálculo do produto desses três fatores: probabilidade versus severidade versus relevância.

   A proposta do cálculo desse critério foi extraída da ferramenta Modulo Risk Manager. Este autor optou pela utilização dessa metodologia de cálculo por entender que os fatores utilizados, bem como suas respectivas escalas de indicadores apresentam conteúdo razoável, sendo reconhecidos e amplamente aceitos em toda a APF. Assim, a seguir, apresentamos o detalhamento de cada fator: sua definição, seus indicadores e algumas boas práticas para as suas respectivas mensurações.

   A probabilidade está diretamente relacionada à possibilidade de que um evento torne indisponível o ativo avaliado. Para esse estudo usamos a tabela 5.14 para estimar esta variável.

Tabela 5.14: Indicadores para o Fator Probabilidade

Probabilidade	**Possibilidade do evento ocorrer**	**Porcentagem esperada**
5 Muito Alta	É praticamente uma certeza	P > 95%
4 Alta	É muito provável	65% < P <= 95%
3 Média	É provável	35% < P <= 65%
2 Baixa	Não é muito provável	5% < P <= 35%
1 Muito Baixa	É pouco provável	P <= 5%

Estimar a probabilidade significa considerar diversos fatores, o que deve ser feito por profissionais de TI que operam com o equipamento. Alguns desses fatores podem ser exemplificados abaixo, mas não se limitam a eles:

- mal funcionamento de componentes internos, devido a sobrecargas de energia elétrica e/ou uso continuado;
- esgotamento da capacidade operacional do equipamento, quer seja de processamento, quer seja de armazenamento;
- para o caso de dispositivos de segurança, como firewalls, ao grau de vulnerabilidade pela falta de atualizações técnicas.

No contexto desse critério, a severidade serve para indicar o nível de impacto no órgão como um todo, caso o ativo TI seja indisponibilizado. Isso significa que, se a interrupção ou mau funcionamento ocorrer, a severidade vai pontuar o grau de comprometimento do desempenho, da confiabilidade ou da qualidade dos ativos do órgão [26].
Os valores utilizados como referência a esse fator podem ser visualizados na tabela 5.15, a seguir:

Tabela 5.15: Indicadores para o Fator Severidade

Severidade	**A ocorrência causará**
5 Muito Alta	Maior comprometimento
4 Alta	Comprometimento muito severo
3 Média	Comprometimento severo
2 Baixa	Comprometimento menos severo
1 Muito baixa	Praticamente não haverá comprometimento

Para estimar a severidade, pode-se usar um ou mais fatores combinados entre si, conforme apresentados a seguir, e devem ser considerados como elementos que poderão influenciar esse valor:

- o grau de comprometimento do desempenho dos ativos, como por exemplo, a produtividade dos processos, serviços embarcados nesses equipamentos;
- o grau de comprometimento da qualidade dos serviços, informações, sistemas ou afins. Por exemplo, a paralização parcial de alguns ativos que podem interromper o fluxo de um pequeno conjunto de informações ou parte do sistema ou do ambiente.

Por fim, completando a especificação do critério Fator de Risco, a relevância deve ser observada, pois ela irá pontuar o nível de importância que o ativo tem para

o órgão, levando em consideração os componentes de negócio que ele suporta. Os valores e regras utilizados para mensuração desse fator pode ser verificado na tabela 5.16, apresentada a seguir: [26].

Tabela 5.16: Indicadores para o Fator Relevância

Relevância	**Comprometimento do ativo**
5 Muito Alta	Poderá afetar todo a organização e as perdas serão extremante altas
4 Alta	Poderá afetar um ou mais negócios da organização e as perdas serão graves
3 Média	Poderá afetar parte dos negócios da organização e as perdas serão consideráveis
2 Baixa	Poderá afetar uma parte pequena e localizada da organização e as perdas serão baixas
1 Muito baixa	Poderá afetar uma parte muito pequena e localizada da organização e as perdas serão mínimas

Assim, após a mensuração dos três componentes do critério em questão, o seu cálculo fica sendo o produto entre esses três componentes e pode ser facilmente visualizado na figura 5.8:

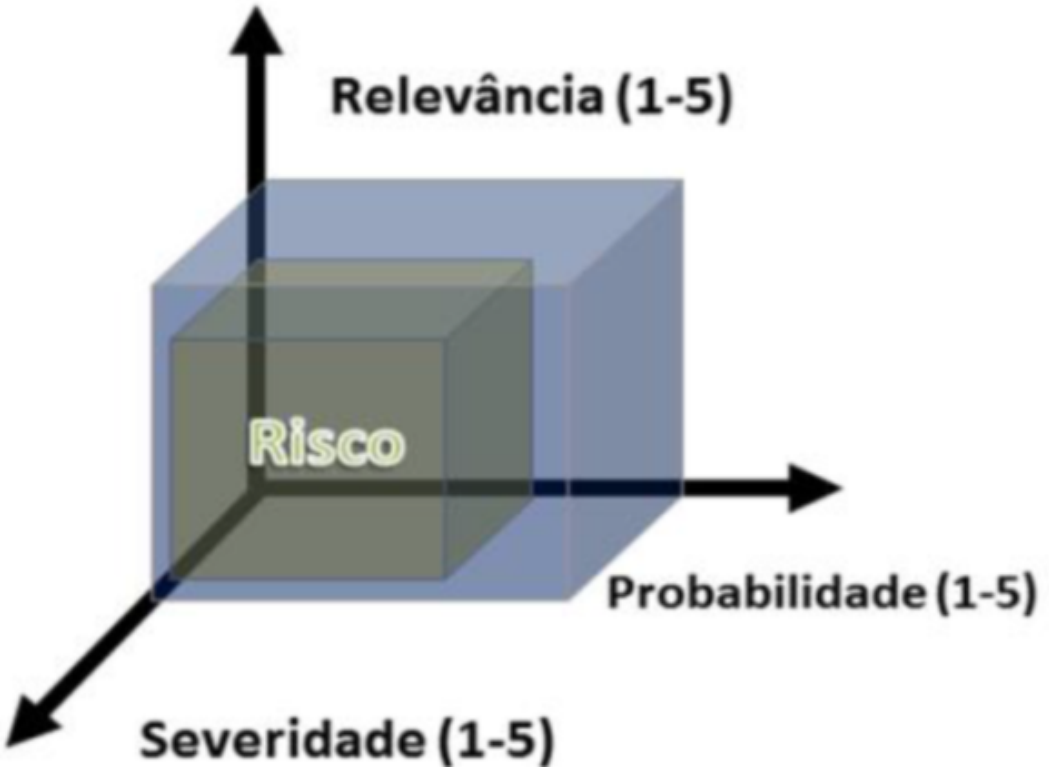

Figura 5.8: Matriz de cálculo do Fator de Risco [26] .

Esse critério é, então, considerado diretamente proporcional à análise de riscos proposta, devido ao grau de importância para o órgão que esse fator irá evidenciar, pois quanto maior for o fator de risco operacional, maior será sua importância no processo decisório proposto, pois os valores obtidos indicam que o ativo de TI, tem extrema valor agregado ao negócio da organização, como um todo.

Assim, após a realização das mensurações e das multiplicações possíveis, foi proposto um conjunto de indicadores para graduar esse critério, e assim poder realizar as etapas seguintes da análise de risco. Foi utilizada a Tabela de Saati [33], que gradua as comparações em escalas de 1, 3, 5, 7 e 9 e, utiliza ainda os valores 2, 4, 6 e 8 como valores intermediários para pequenos ajustes.

Os valores propostos para esse indicador estão discriminados, conforme explicitado na tabela 5.17:

Tabela 5.17: Indicadores do Critério: Fator de risco operacional

Critério: Fator de risco operacional	**Valor**
75 – 80 – 100 – 125	9
50 – 60 – 64	8
40 – 45 – 48	7
30 – 32 – 36	6
24 – 25 – 27	5
16 – 18 – 20	4
10 – 12 – 15	3
6 – 8 – 9	2
1 – 2 – 3 - 4 – 5	1

6. Capacidade Operacional do Ativo Segundo Rodrigues [31], a biblioteca Information Technology Infrastructure Library (ITIL) define capacidade como sendo o rendimento máximo que um item de configuração ou um serviço de TI pode entregar, ao mesmo tempo em que cumpre os níveis de serviço acordados.

   No contexto dessa pesquisa, foi considerada a capacidade operacional do ativo de TI como a magnitude ou o limite de utilização desse ativo, no qual o equipamento ou software consegue entregar resultados.

   Esse cálculo é realizado, principalmente, como resultado de uma avaliação técnica que possa definir a taxa de uso de um determinado ativo de TI que varia de ativo para ativo, em tipo, métrica e resultados.

   A fim de ilustrar as possibilidades, ou melhor, a diversidade de formas de se computar esse critério, pode-se citar o exemplo de um equipamento do tipo storage, que terá sua capacidade operacional esgotada quando atingir o limite de espaço de arma-

zenamento em disco. Outro exemplo seria a capacidade operacional de um servidor de rede que se esgotará quando atingir o limite de capacidade de processamento; e assim por diante.
A fim de criar um indicador para esse critério, foi idealizada uma fórmula que apresenta a porcentagem remanescente da capacidade operacional remanescente. Esse cálculo é realizado, de acordo com a fórmula a seguir:

$$Porcentagem\ da\ Capacidade\ Operacional\ Remanescente = 1{,}00 - \frac{Taxa\ de\ uso\ atual}{Cap.\,Op.\,Padrão}$$

Figura 5.9: Fórmula de Capacidade operacional .

Uma vez realizados os cálculos necessários para o levantamento desse critério, considerou-se nessa pesquisa que essa porcentagem da capacidade operacional do ativo remanescente é inversamente proporcional à análise de riscos proposta, porque quanto maior for a capacidade operacional disponível, menor será sua importância no processo decisório proposto, pois subentende-se que dispositivos com pouco uso, ou pouca taxa de ocupação não necessitem de atualização, upgrade ou modernização.
Assim, a fim de criar um indicador para graduar esse critério, e desta forma poder realizar as etapas seguintes da análise de riscos proposta, foi utilizada a Tabela de Saati [33], que gradua as comparações em escalas de 1, 3, 5, 7 e 9 e, utiliza ainda os valores 2, 4, 6 e 8 como valores intermediários para pequenos ajustes.
Dessa forma, os indicadores para esse critério podem ser visualizados na tabela 5.18, descrita a seguir:

Tabela 5.18: Indicadores do Critério: Capacidade operacional do ativo de TI

Critério: Capacidade operacional do ativo de TI	**Valor**
Até de 20%	9
Acima de 20% até 30%	8
Acima de 30% até 40%	7
Acima de 40% até 50%	6
Acima de 50% até 60%	5
Acima de 60% até 70%	4
Acima de 70% até 80%	3
Acima de 80% até 90%	2
Acima 90%	1

5.2.7 Operação do sistema proposto

Agora que os critérios para o processo de análise foram definidos, é necessário inserir os dados no sistema para que sejam utilizados. Na tabela 5.19, pode-se verificar as informações necessárias para otimização dos critérios, bem como suas respectivas fontes.

Tabela 5.19: Fontes das informações necessárias à análise de risco

Informações Necessárias	**Fonte de origem**
1 Preço de Atendimento "Per call"	Fornecedores de Soluções de TI
2 Preço do Contrato Individualizado	Fornecedores de Soluções de TI
3 Contrato Anual	Fornecedores de Soluções de TI – Contrato atual
4 Orçamento Anual do Setor	Ordenador de Despesas da Organização
5 Preço global do produto	Fornecedores de Soluções de TI – Nota Fiscal
6 Patrimônio de TI da Organização	Gestor de TI da Organização
7 Tempo de Uso da Solução de TI	Gestor de TI da Organização
8 Tempo de Vida Útil da Solução de TI	Fornecedores de Soluções de TI
9 Probabilidade da Solução de TI (Parar)	Equipe técnica da Organização
10 Severidade da Solução de TI	Equipe técnica da Organização
11 Impacto da Solução de TI	Equipe técnica da Organização
12 Taxa de Uso da Solução de TI	Equipe técnica da Organização
13 Capacidade Operacional Padrão da Solução de TI	Fornecedores de Soluções de TI

De acordo com a IN nº 5, de 27 de junho de 2014, da SLTI, que dispõe sobre os procedimentos administrativos básicos para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, as informações que são provenientes dos fornecedores de soluções de TI devem ser formalmente requisitadas, através de canais de comunicação como ofícios e/ou mensagens eletrônicas (e-mails), para que possam ser utilizadas em um processo formal de contratação [9].

Diante dessa premissa estabelecida pela IN 05/SLTI/2014, o sistema deve emitir mensagens automaticamente aos fornecedores de soluções de TI solicitando aquelas informações que lhe são afetas.

Uma vez que todas as informações foram coletadas, elas serão inseridas no sistema pelo gestor de TI e quando concluída essa etapa, todos os ativos terão seus indicadores estabelecidos e pode-se então, iniciar o processo de análise de riscos de investimento de TI.

A análise pode ser conduzida com tantos critérios quanto sejam necessários. O sistema deve prover ao gestor, a possibilidade de selecionar quais critérios devem ser utilizados no processo.

Assim como os critérios, o sistema deve prover ao gestor a escolha de quais ativos de TI

devem participar da análise.
Uma vez que os critérios e ativos de TI e foram selecionados, o sistema possibilitará ao gestor fazer uma comparação par a par com os critérios, que serão dispostos numa matriz quadrada. Cada par avaliado receberá um valor que varia de 1 a 9 e, o sistema deverá calcular, automaticamente, a avaliação para o par inverso. A conclusão dessa atividade proverá ao sistema, o peso que cada critério terá na análise proposta.
Diversos cenários podem ser montados, adicionando ou removendo critérios da análise. No entanto, é relevante destacar que cada alteração (inclusão, modificação ou exclusão de critérios na análise) forçará o gestor a fazer uma nova comparação par a par com esse novo conjunto de critérios.
Na figura 5.10, pode ser visto uma matriz quadrada simulando a comparação par a par com quatro critérios selecionados. Nesse quadro, as células na cor "azul" que delimitam a diagonal principal da Matriz, sempre terão o valor igual a "1", pois a comparação de um critério contra ele mesmo, será sempre igual à unidade. As células na cor "branca" serão preenchidas pelo gestor de TI, de acordo com o grau de relevância que um critério tenha para o processo como um todo quando comparado a outro critério. Por fim, as células delimitadas em negrito e na cor "verde" serão preenchidas automaticamente pelo sistema, pois são os campos que representam as comparações inversas daquelas que foram feitas pelo gestor de TI. Os valores dessas células serão os inversos daqueles lançados nas células na cor "branca".

COMPARAÇÃO	CRITÉRIO 01	CRITÉRIO 02	CRITÉRIO 03	CRITÉRIO 04
CRITÉRIO 01				
CRITÉRIO 02				
CRITÉRIO 03				
CRITÉRIO 04				

Figura 5.10: Modelo de Matriz de Comparação de Critérios .

Após os valores serem lançados no sistema, este deve, automaticamente, realizar as seguintes etapas:

- Normalização da matriz de comparação: Esta tarefa é realizada através da soma dos valores de cada coluna da matriz de comparação. Posteriormente, cada valor da coluna é dividido pelo somatório obtido nessa mesma coluna;

- Cálculo do vetor de Eigen: nesta etapa o objetivo é o de identificar um vetor de prioridades global que armazene a prioridade associada a cada alternativa em relação ao foco principal. Esse vetor é calculado através da média aritmética das linhas da matriz de comparação após a etapa de normalização;
- Consistência lógica: Verificação da coerência entre as atribuições dos valores atribuídos pelo gestor de TI a cada comparação. Esse cálculo (RC) é feito pela seguinte razão IC/IR, onde IR é o Índice de Consistência Randômico obtido para uma matriz recíproca de ordem n, com elementos não-negativos e gerada randomicamente e o Índice de Consistência (IC) é dado por λ – n)/(n - 1), onde λ máx calculado através da soma dos produtos entre cada valor do Vetor de Eigen e pelo total da respectiva coluna da matriz de comparação original [33].

Segundo Saaty (2005) a condição de consistência da matriz de Comparação é aceitável se o valor de RC for menor ou igual a 0,10, ou seja, se RC $\leqslant$ 0,10. Vale lembrar que o valor de IR é fixo e foi definido por Saaty numa tabela própria [33].
Vencida essa etapa, inicia-se a análise par a par dos ativos de TI, tomando por base um único critério. Essa nova fase do processo é de extrema importância e será repetida para todos os critérios selecionados para a análise.
O sistema deve montar uma matriz quadrada com os ativos de TI, semelhante à matriz do processo anterior, só que os ativos devem ser comparados, tendo como referência cada um dos critérios selecionados. Usando a quantidade de critérios sugerida na tabela anterior, essa etapa teria então, quatro matrizes, e o processo de preenchimento seria semelhante ao utilizado quando da etapa de comparação de critérios.
As células em "azul" teriam o valor "1". Aquelas em "verde" serão preenchidas pelo Gestor de TI e as células em "laranja" serão preenchidas automaticamente pelo sistema, com os valores inversos àqueles lançados nas células "verde".
Agora na figura 5.11, pode ser visto uma matriz quadrada simulando a comparação par a par de cinco ativos de TI. Deve-se notar que a célula inicial (analogamente, no software Microsoft excel, seria a posição A1) verifica-se que está destacado o Critério 01. Ato contínuo, a matriz seguinte seria com o Critério 02, depois o Critério 03 e, assim sucessivamente até que sejam feitas todas as comparações, com todos os critérios selecionados para a análise.
Nesta figura, as células na cor "azul" que delimitam a diagonal principal da Matriz, sempre terão o valor igual a "1", pois a comparação de um ativo contra ele mesmo, será sempre igual à unidade. As células na cor "branca" serão preenchidas pelo gestor de TI, de acordo com os indicadores pré-concebidos anteriormente. Importante lembrar que nessa etapa os ativos de TI são comparados entre si, par a par, tomando como referência um único critério. Por fim, as células delimitadas em negrito e na cor "verde" serão preenchidas au-

tomaticamente pelo sistema, pois são os campos que representam as comparações inversas daquelas que foram feitas pelo gestor de TI. Os valores dessas células serão os inversos daqueles lançados nas células na cor “branca”.

CRITÉRIO 01	ATIVO 01	ATIVO 02	ATIVO 03	ATIVO 04	ATIVO 05
ATIVO 01					
ATIVO 02					
ATIVO 03					
ATIVO 04					
ATIVO 05					

Figura 5.11: Modelo de Matriz quadrada de Análise de Ativos de TI por Critério .

Essas matrizes, seguindo o mesmo raciocínio da primeira matriz, a matriz de critérios, também devem ser normalizadas e, o processo é idêntico ao descrito na etapa de normalização daquela matriz.
Vencida essa etapa, a etapa seguinte é a consolidação de todas as avaliações. Esse processo é feito de forma automática pelo sistema e, ele ocorre da seguinte forma:
Na matriz de comparação dos critérios, foram registrados os valores do Vetor de Eigen para cada critério considerado.
Nas matrizes seguintes, após a normalização, obtém-se a média de cada linha que é considerado o peso que aquele critério tem, sobre o processo decisório.
O cálculo por ativo será feito através do somatório dos produtos entre o peso de prioridade do ativo de TI e o peso do critério que foi determinado pelo Vetor de Eigen.
Ao término, o sistema apresentará um relatório, ordenado de forma decrescente, pelo percentual obtido pelos ativos de TI. Essa relação indicará a prioridade de investimentos à luz dos critérios estabelecidos. O ativo de TI que obtiver o maior percentual, será o de maior prioridade.

5.2.8 Mapeamento do processo de contratação de TI no DSIC (Fluxo proposto)

Nesta etapa foi mapeado o processo de contratação de TI do DSIC. Como ele será após a implementação da solução proposta. Este mapeamento é conhecido como Modelo “To Be”, pois retrata como o processo ficará após o sistema ser posto em produção.
Ele está simbolicamente apresentado na figura 5.12, a seguir, porém, pode ser melhor visualizado em tamanho ampliado, no Apêndice C.

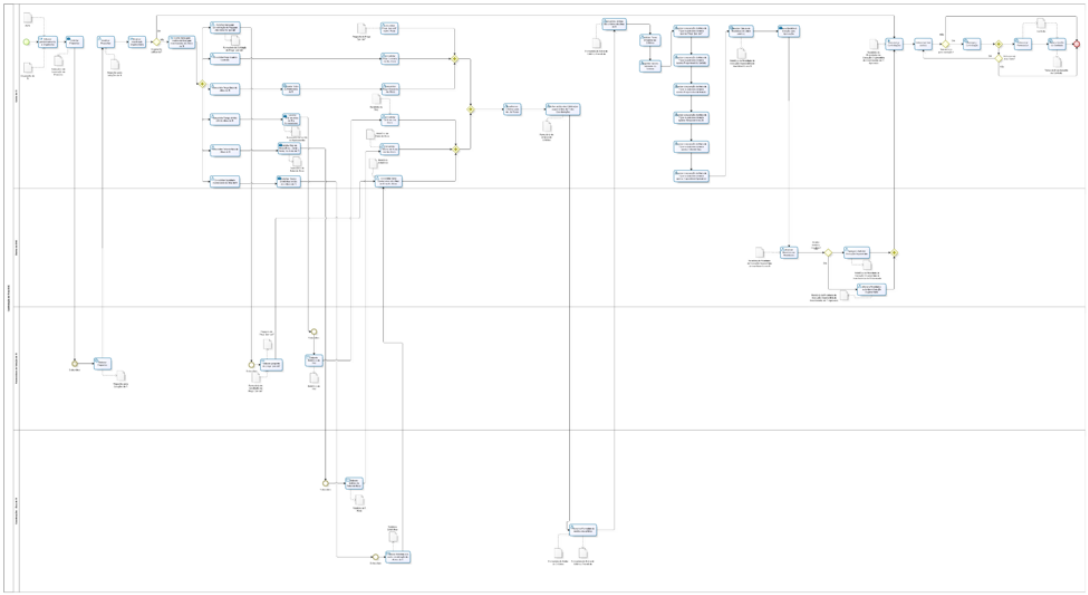

Figura 5.12: Mapeamento do Processo de Contratação de TI (DSIC) "To Be".

- Descrição das Atividades, gateways e raias do Mapeamento:
  Neste ponto, serão descritas as atividades desenhadas no mapeamento, assim como os gateways e raias que simbolizam os atores do processo proposto. Observe que a descrição segue o fluxo do processo, da forma mais linear possível.

  1. Atividade: Estudar preliminarmente o Orçamento
     O Gestor de TI analisa o PDTI e o Orçamento previsto da Organização.
  2. Atividade: Estudar preliminarmente o Orçamento
     O Gestor de TI analisa o PDTI e o Orçamento previsto da Organização.
  3. Atividade: Solicitar Propostas
     O Gestor de TI solicita aos fornecedores das diversas soluções de TI uma proposta para a atividade prevista no PDTI (Manutenção, Aquisição, Atualização Evolutiva, etc.) através de documento formal, gerado pelo sistema.

4. Atividade: Elaborar Propostas
   Os fornecedores elaboram e enviam ao Gestor de TI as propostas solicitadas, podendo essas propostas serem de manutenção, atualização ou aquisição.
5. Atividade: Analisar Propostas
   Após receber as propostas dos fornecedores, o Gestor de TI analisa e seleciona o preço-base para ser utilizado como valor de referência para estudos e/ou processo de contratação.
6. Atividade: Analisar Viabilidade Orçamentária
   Após consolidar todos os preços e popular com os dados das propostas de todos os ativos de TI, o Gestor de TI verifica se há orçamento suficiente para a execução de todas as atividades previstas no PDTI.
7. Gateway: Orçamento suficiente?
   Sim: Ir para a atividade “Executar as Contratações”.
   Não: Ir para a atividade “Coletar dados para Análise de Risco para Investimento em Ativos de TI”.
8. Atividade: Coletar dados para Análise de Risco para Investimento em Ativos de TI
   Início de uma sequência de atividades para coleta de dados para popular a ferramenta de análise de riscos em investimentos em TI.
9. Atividade: Solicitar dados para consolidação de Preço para Atendimento "per call"
   Solicitar, através de documento oficial, aos fornecedores de soluções de ativos de TI o preço médio para atendimento “per call” de sua solução.
10. Atividade: Elaborar propostas de preço "per call"
    Os fornecedores elaboram e enviam ao Gestor de TI os preços médios de atendimento “per call” de suas soluções de ativos de TI.
11. Atividade: Consolidar Preço "per call"na Análise de Riscos
    O Gestor de TI cadastra no Sistema os dados obtidos para cálculo do indicador para esse critério. Essas informações apresentarão como resultado qual a porcentagem que o preço “per call” representa em relação ao valor do contrato de manutenção do ativo de TI. Essa porcentagem então, é comparada a um quadro previamente cadastrado que informa os indicadores desse critério.
12. Atividade: Consolidar Preço Anual do Contrato
    O Gestor de TI busca as informações necessárias ao cadastramento no sistema para consolidação do preço anual do contrato. Essas informações são obtidas, ou pelo contrato em vigor, fazendo-se uma projeção de reajuste com base em

sua cláusula de reajuste, ou pelo orçamento obtido nas propostas iniciais enviadas aos fornecedores quando das solicitações feitas pela atividade “Solicitar propostas”.

13. Atividade: Consolidar Preço do Contrato na Análise de Riscos
    O Gestor de TI cadastra no Sistema os dados obtidos para cálculo do indicador para esse critério. Essas informações apresentarão como resultado qual a porcentagem que o preço do contrato anual representa em relação ao valor do orçamento anual para gestão de TI. Essa porcentagem então, é comparada a um quadro previamente cadastrado que informa os indicadores desse critério.
14. Atividade: Consolidar Preço Global do Ativo de TI
    O Gestor de TI consolida o valor total das soluções implementadas. Cada ativo tem seu preço unitário cadastrado. Essa consolidação faz um somatório dos preços unitários, quando os ativos são agrupados. Contratos, quando estabelecidos, são firmados para todos os ativos de uma determinada marca/modelo, por isso a consolidação do preço global do ativo de TI.
15. Atividade: Calcular Valor do Patrimônio de TI
    O Gestor de TI consolida a soma de todos os ativos de TI cadastrados no sistema de forma a calcular o valor total do patrimônio de TI da Organização.
16. Atividade: Consolidar Preço Global na Análise de Riscos
    O Gestor de TI consolida o preço global das soluções implementadas. Essas informações apresentarão como resultado qual a porcentagem que o preço global da solução de TI representa em relação ao patrimônio total de TI da Organização. Essa porcentagem então, é comparada a um quadro previamente cadastrado que informa os indicadores desse critério.
17. Atividade: Consolidar Tempo de Vida Útil do Ativo de TI
    O Gestor de TI busca as informações necessárias ao cadastramento no sistema para consolidação do Tempo de Vida Útil do Ativo de TI. Essas informações são obtidas através dos fornecedores das soluções de TI.
18. Atividade: Solicitar Tempo de Vida Útil do Ativo de TI a Fornecedores
    O Gestor de TI solicita aos fornecedores das diversas soluções de TI as especificações dos seus produtos, descrevendo em detalhes os seus tempos estimados de vida útil através de documento formal, gerado pelo sistema.
19. Atividade: Elaborar Relatório de Tempo de Vida Útil
    Os fornecedores enviam ao Gestor de TI os relatórios com os tempos de vida útil estimados de suas soluções de TI.

20. Atividade: Consolidar Tempo de Vida Útil na Análise de Riscos
    O Gestor de TI, de posse do relatório, analisa, caso a caso, as soluções de TI existentes e, de acordo com o plano de depreciação da STN, aplica a depreciação prevista para cada ativo de TI. Esse processo é concluído com percentual de tempo de vida útil remanescente do ativo de TI. Esse percentual é então aplicado ao quadro de indicadores deste critério e seu valor armazenado para uso na análise de riscos, em si.
21. Atividade: Consolidar Fator de Risco do Ativo de TI
    O Gestor de TI requisita as informações necessárias ao cadastramento no sistema do fator de risco do Ativo de TI. Essas informações são obtidas através da área técnica das Coordenações, que são os usuários diretos das soluções de TI.
22. Atividade: Solicitar Fator de Risco (Probabilidade – Severidade – Relevância) às Áreas de TI
    O Gestor de TI solicita aos responsáveis técnicos das Coordenações do Departamento os valores necessários ao cálculo do fator de risco, a saber, probabilidade, severidade e relevância, todos medidos numa escala de 1 a 5. Essa solicitação é feita através de um formulário online onde o responsável, ao responder, já estará inserindo tais informações no sistema.
23. Atividade: Elaborar Índices de Fator de Risco
    Os representantes técnicos das áreas de TI responderão um questionário online enviado pelo sistema. Para cada ativo de TI sob sua responsabilidade devem ser preenchidos valores de 1 a 5 nos fatores de riscos (probabilidade, severidade e relevância).
24. Atividade: Consolidar Fatores de Risco na Análise de Riscos
    O Gestor de TI analisará os resultados enviados pelos representantes técnicos e determinará quais fatores devem ser considerados para uma determinada solução de TI. Deve-se observar que três ativos de TI de mesma marca e modelo podem, de acordo com os serviços embarcados, apresentarem fatores de risco distintos e, nesse caso, o gestor de TI deve consolidar esses fatores e determinar qual deles será utilizado na análise de riscos.
25. Atividade: Consolidar Capacidade Operacional do Ativo de TI
    O gestor de TI requisita as informações necessárias ao cadastramento no sistema da capacidade operacional de cada ativo de TI. Essas informações são obtidas através da área técnica das Coordenações, que são os usuários diretos das soluções de TI.

26. Atividade: Solicitar Dados Estatísticos de Uso dos Ativos de TI
    O gestor de TI solicita aos responsáveis técnicos das Coordenações do Departamento as taxas de uso de cada ativo sob sua responsabilidade, como por exemplo, espaço disponível em uso do disco rígido, taxa de uso da CPU, dentre outros. Essa solicitação pode ser feita através de um formulário próprio.
27. Atividade: Elaborar Relatório com dados de utilização dos Ativos de TI
    Os representantes técnicos das áreas de TI responderão o formulário. Para cada ativo de TI sob sua responsabilidade devem ser preenchidos os dados operacionais dos equipamentos.
28. Atividade: Consolidar Dados Operacionais dos Ativos de TI na Análise de Riscos
    O gestor de TI analisará os resultados enviados pelos representantes técnicos e determinará quais dados devem ser considerados para uma determinada solução de TI. Deve-se observar que três ativos de TI de mesma marca e modelo podem, de acordo com os serviços embarcados, apresentarem capacidades operacionais distintas e, nesse caso, o gestor deve consolidar esses valores e determinar qual será utilizado na análise de risco.
29. Atividade: Escolher os Critérios para Análise de Riscos
    O sistema permite o cadastramento de diversos critérios e neste momento, o gestor de TI deve determinar quais critérios devem ser utilizados na análise de riscos.
30. Atividade: Solicitar análise dos Critérios (par a par) à Área de TI das Coordenações
    O gestor de TI solicita aos representantes técnicos da área de TI das Coordenações para estabelecer os pesos que cada critério terá sobre a análise de riscos, como um todo.
31. Atividade: Preencher Formulário de Análise dos critérios
    Os representantes técnicos das áreas de TI das Coordenações preencherão os formulários enviados com suas opiniões sobre as avaliações de critérios par a par.
32. Atividade: Consolidar Análises dos critérios das Áreas de TI
    O gestor de TI consolida os dados obtidos pelos formulários enviados pelos responsáveis técnicos das áreas de TI das Coordenações.
33. Atividade: Validar Pesos atribuídos aos Critérios
    O gestor de TI analisa os dados consolidados e determina os valores finais a serem lançados no sistema.

34. Atividade: Registrar valores validados no Sistema
    O gestor de TI registra no sistema, os valores consolidados, analisados e validados. O sistema então, realiza os cálculos necessários para estabelecimento dos pesos que cada critério tem no processo, como um todo. Estes pesos são identificados no processo como o "Vetor de Eigen". As atividades seguintes, de realização de comparação de ativos, serão opcionais, pois somente acontecerão se o critério for selecionado para a análise de riscos.
35. Atividade: Realizar comparação de Ativos de TI (par a par) considerando apenas Preço "per call"
    O gestor de TI realiza a análise dos ativos de TI, par a par, tomando como referência o Preço de atendimento "per call". Esse critério possui indicadores estabelecidos e cada ativo de TI já tem seu respectivo indicador. A análise dos ativos de TI é montada sob forma de fração com os indicadores previamente estabelecidos de cada equipamento.
36. Atividade: Realizar comparação de Ativos de TI (par a par) considerando apenas Preço Anual do Contrato
    O gestor de TI realiza a análise dos ativos de TI, par a par, tomando como referência o Preço Anual do Contrato. Esse critério possui indicadores estabelecidos e cada ativo de TI já tem seu respectivo indicador. A análise dos ativos de TI é montada sob forma de fração com os indicadores previamente estabelecidos de cada equipamento.
37. Atividade: Realizar comparação de Ativos de TI (par a par) considerando apenas Preço Global do Produto
    O gestor de TI realiza a análise dos ativos de TI, par a par, tomando como referência o Preço Global do Produto. Esse critério possui indicadores estabelecidos e cada ativo de TI já tem seu respectivo indicador. A análise dos ativos de TI é montada sob forma de fração com os indicadores previamente estabelecidos de cada equipamento.
38. Atividade: Realizar comparação de Ativos de TI (par a par) considerando apenas Tempo de Vida Útil
    O gestor de TI realiza a análise dos ativos de TI, par a par, tomando como referência o Tempo de Vida Útil. Esse critério possui indicadores estabelecidos e cada ativo de TI já tem seu respectivo indicador. A análise dos ativos de TI é montada sob forma de fração com os indicadores previamente estabelecidos de cada equipamento.
39. Atividade: Realizar comparação de Ativos de TI (par a par) considerando

apenas fator de Risco

O gestor de TI realiza a análise dos ativos de TI, par a par, tomando como referência o Fator de Risco. Esse critério possui indicadores estabelecidos e cada ativo de TI já tem seu respectivo indicador. A análise dos ativos de TI é montada sob forma de fração com os indicadores previamente estabelecidos de cada equipamento.

40. Atividade: Realizar comparação de Ativos de TI (par a par) considerando apenas Capacidade Operacional

    O gestor de TI realiza a análise dos ativos de TI, par a par, tomando como referência a capacidade operacional. Esse critério possui indicadores estabelecidos e cada ativo de TI já tem seu respectivo indicador. A análise dos ativos de TI é montada sob forma de fração com os indicadores previamente estabelecidos de cada equipamento.

41. Atividade: Realizar Cálculos de Prioridade (Análise Multicritério)

    O sistema efetua então, os cálculos para o estabelecimento da lista de prioridades de ativos de TI. Essa atividade é feita através do somatório dos produtos entre o peso da prioridade do ativo de TI e o peso do critério que foi determinado na atividade "Registrar valores validados no Sistema".

42. Atividade: Enviar Relatório à Direção para Aprovação

    Uma vez concluída a atividade "Realizar Cálculos de Prioridade (Análise Multicritério)", o seu resultado é uma lista dos ativos de TI e seus respectivos percentuais. Esses percentuais representam o índice de risco para investimento de TI. Quanto maior o valor encontrado, maior será a indicação para que o investimento seja feito. Esse processo gera um relatório, relacionando os ativos em ordem decrescente de prioridade. Esse relatório é, então, enviado ao Diretor do Departamento para análise e aprovação.

43. Atividade: Analisar Relatório de Prioridades

    O Diretor do Departamento recebe o relatório para análise e aprovação.

44. Gateway: O Diretor realizou ressalvas?

    Sim: Ir para a atividade "Alterar a prioridade e autorizar a execução orçamentária".

    Não: Ir para a atividade "Aprovar e autorizar a execução orçamentária".

45. Atividade: Aprovar e Autorizar Execução Orçamentária

    O Diretor do Departamento aprova e autoriza a execução das contratações, de acordo com a prioridade apresentada.

46. Atividade: Alterar a Prioridade e autorizar a Execução Orçamentária

O Diretor do Departamento altera a prioridade apresentada e autoriza a execução das contratações, de acordo com a nova prioridade.

47. Atividade: Executar as Contratações
    O gestor de TI realiza o processo de contratação, à luz da IN 04/2014, da SLTI.
48. Atividade: Selecionar item da lista
    É feita a seleção do primeiro item da lista prioridades que foi aprovada pela Direção do Departamento.
49. Gateway: Tem recurso orçamentário para execução?
    Sim: Ir para a atividade "Planejar a contratação".
    Não: Ir para o fim do processo.
50. Atividade: Planejar a Contratação
    Planejar a contratação é, na verdade, um subprocesso que está exemplificado na figura 5.13 e, não será detalhado, por estar fora do escopo da presente pesquisa:

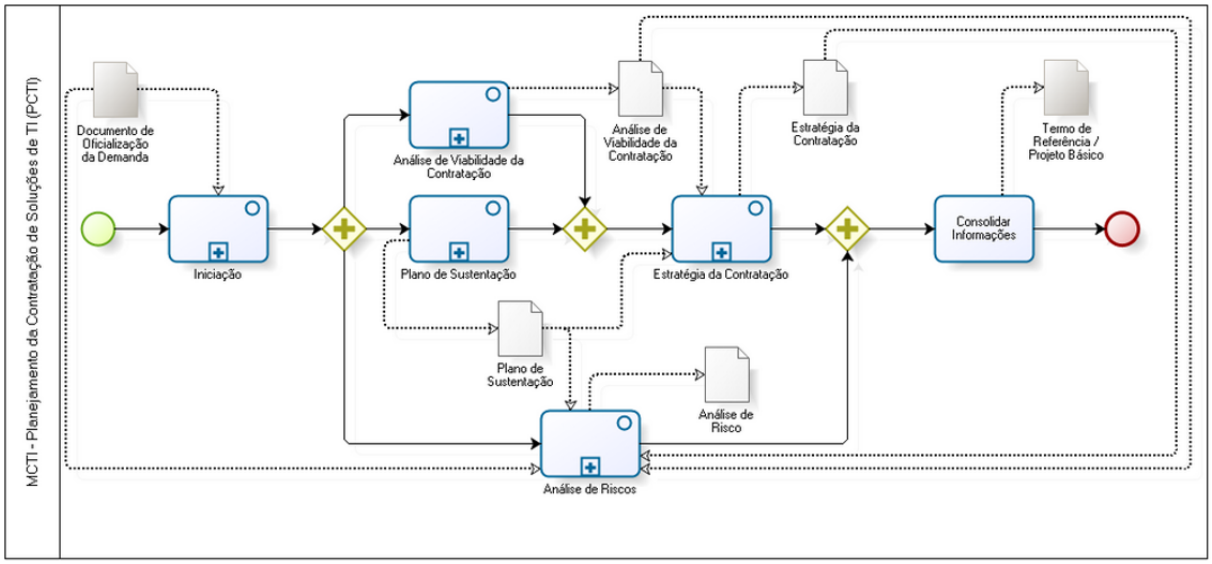

Figura 5.13: Mapeamento do Processo de Contratação de TI [8].

Esse subprocesso possui cinco subprocessos, que estão ilustrados nas figuras 5.14 a 5.18, a seguir:

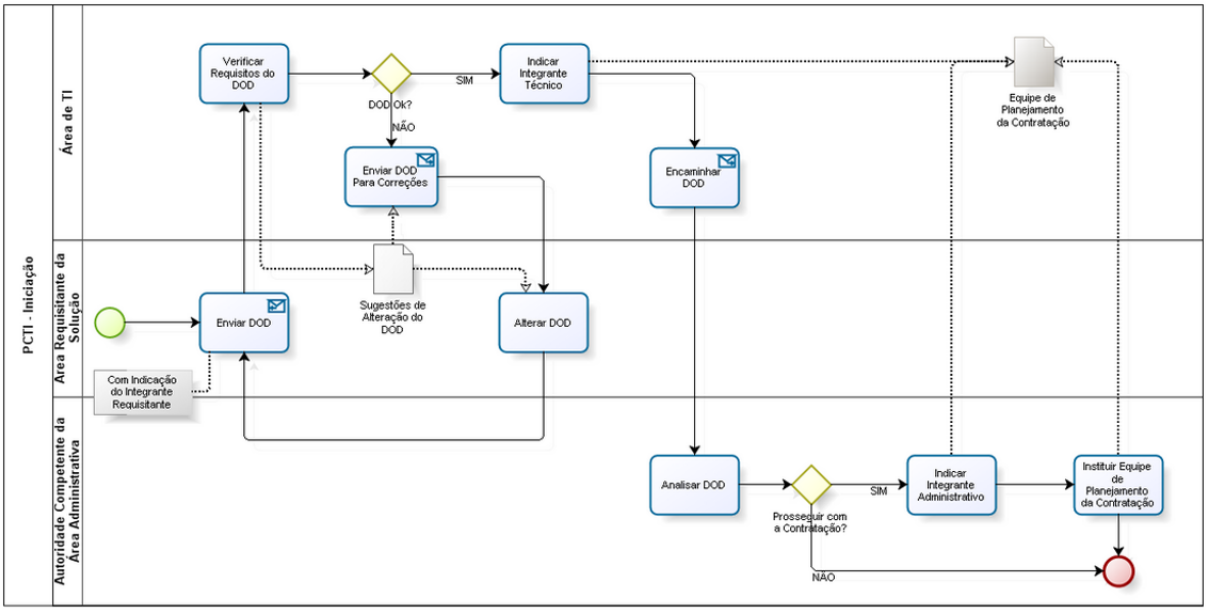

Figura 5.14: Mapeamento do Processo "Iniciação"do Processo de Contratação de TI [8].

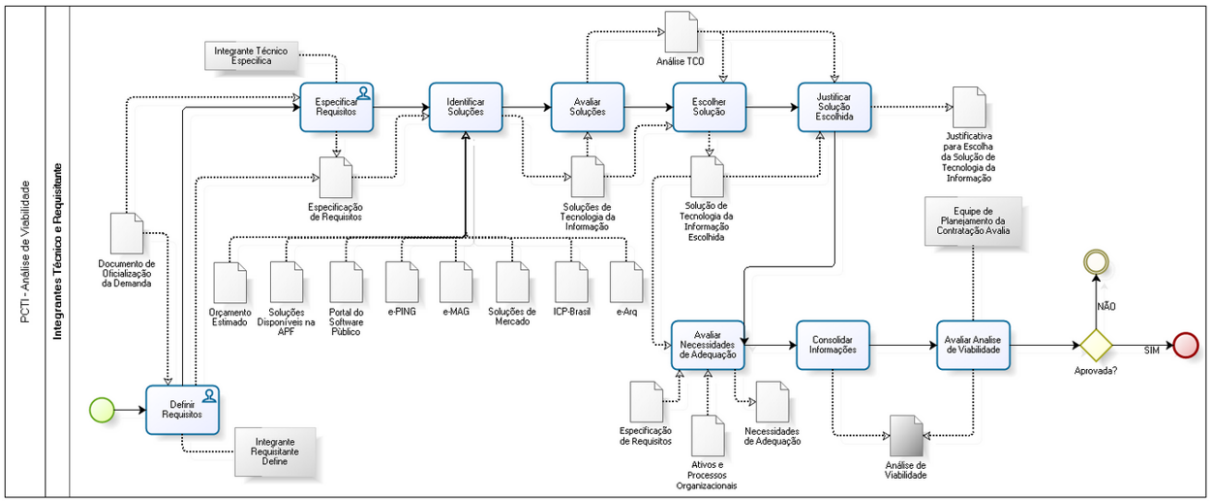

Figura 5.15: Mapeamento do processo "Análise de viabilidade"do Processo de Contratação de TI [8] .

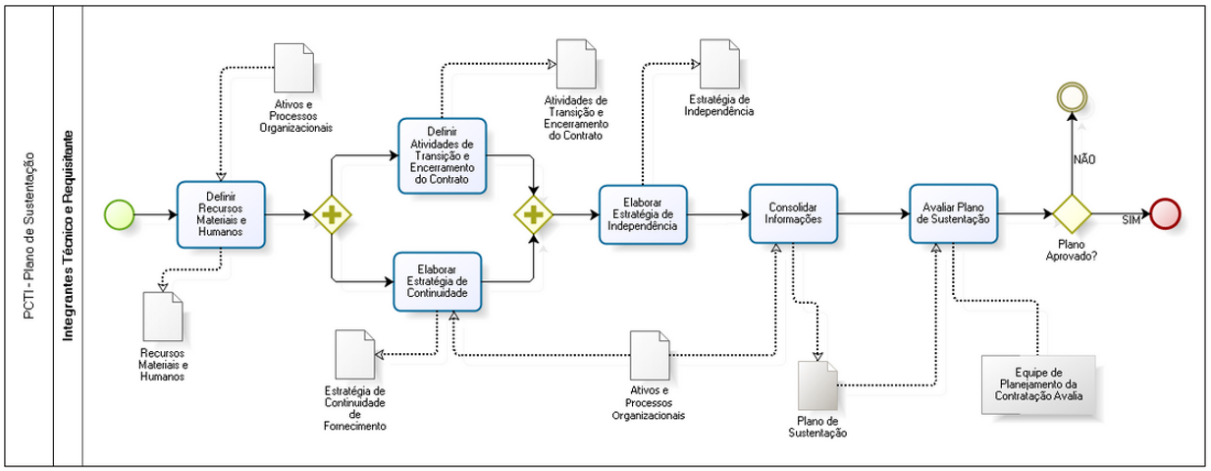

Figura 5.16: Mapeamento do processo “Plano de Sustentação"do Processo de Contratação de TI [8] .

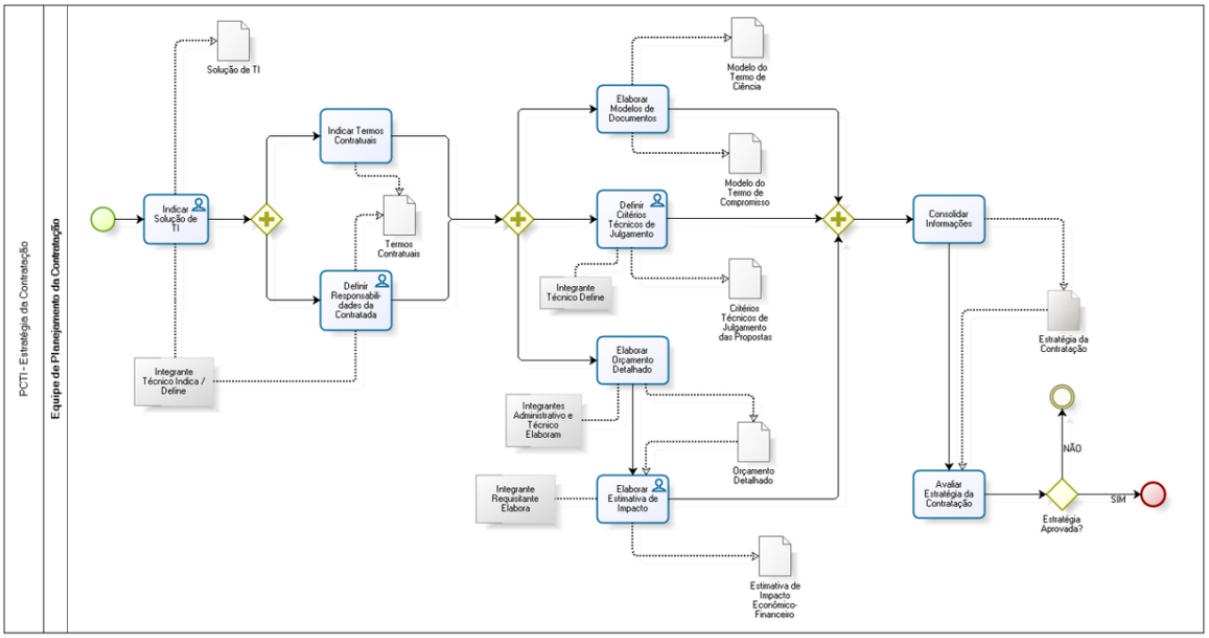

Figura 5.17: Mapeamento do processo "Estratégia da Contratação"do Processo de Contratação de TI [8] .

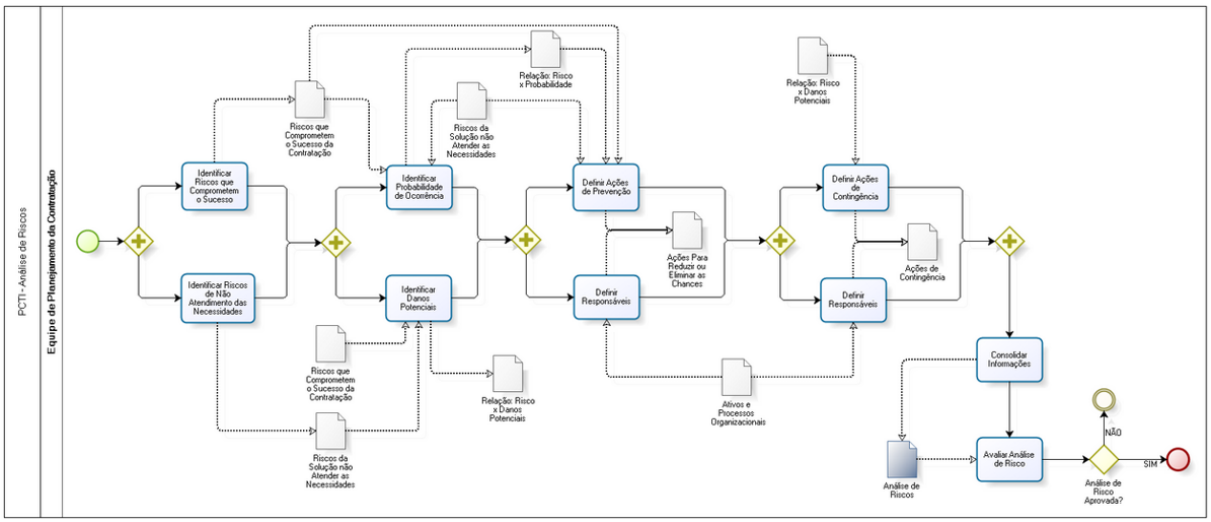

Figura 5.18: Mapeamento do processo "Análise de Risco"do Processo de Contratação de TI [8] .

51. Gateway: Lista de Execução possui mais itens?
    Sim: Ir para a atividade “Selecionar item da lista”.
    Não: Ir para o fim do processo.

52. Atividade: Selecionar Fornecedor
    Esta atividade é, na verdade, outro subprocesso de licitação e ele é detalhado conforme mapeamento abaixo. Esta atividade não faz parte do escopo da pesquisa e, portanto, será apenas apresentada o seu mapeamento na figura 5.19.

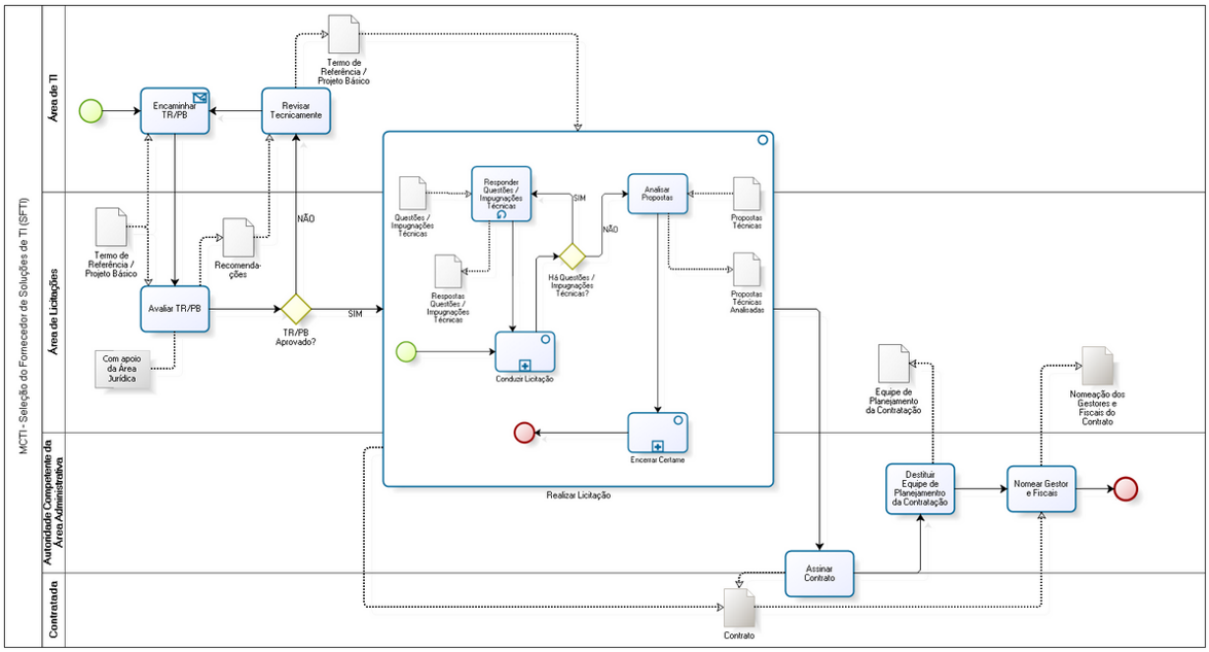

Figura 5.19: Mapeamento do Processo "Seleção do Fornecedor"do Processo de Contratação de TI [8] .

53. Atividade: Fazer a Gestão do Contrato

    A atividade “Fazer a Gestão do Contrato” é detalhado conforme mapeamento abaixo. Assim como as atividades anteriores, essa atividade também é um sub-processo e, também não faz parte do escopo desta pesquisa e, portanto, nesta etapa ela será apenas apresentada na figura 5.20, através de seu mapeamento.

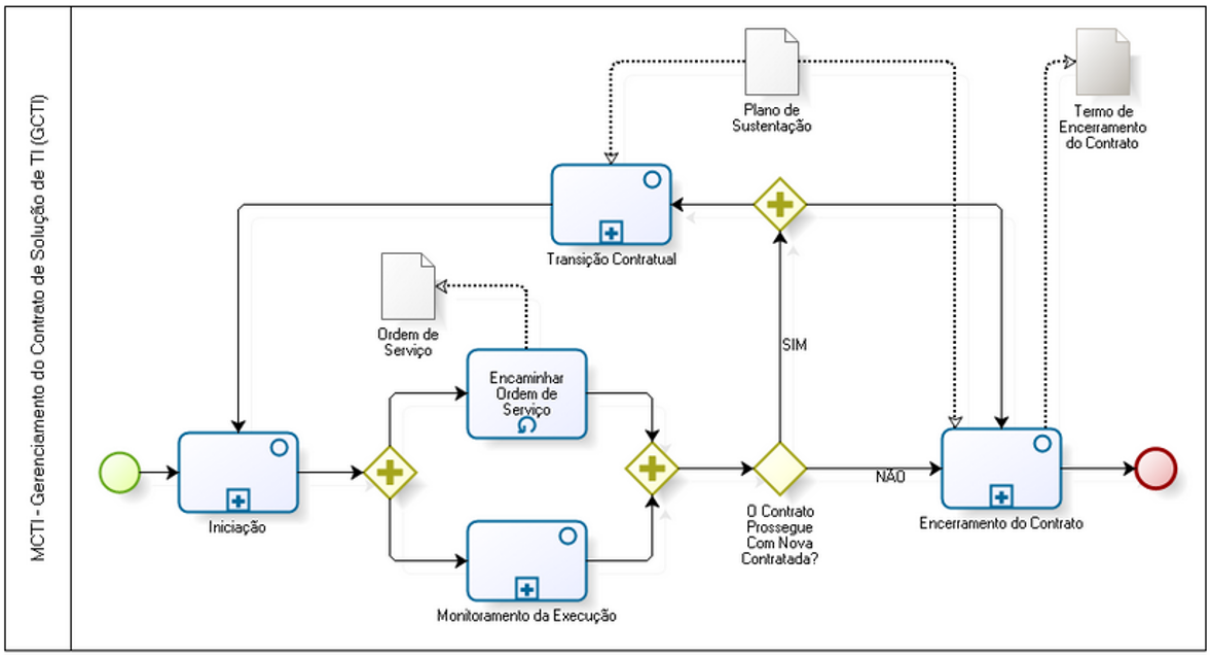

Figura 5.20: Mapeamento do Processo "Gestão do Contrato"do Processo de Contratação de TI [8] .

54. Raia: Gestor de TI
    Representa não só o gestor, mas toda a equipe de gestão de recursos de TI.
55. Raia: Diretor do DSIC
    Representa a Direção do Departamento.
56. Raia: Fornecedores de Solução de TI
    Representa todo o universo de empresas que fornece soluções de TI ao DSIC.
57. Raia: Coordenações – Área de TI
    Representa as três Coordenações finalísticas do DSIC: a CGGSIC, a CGSSC e a CGTIR.

5.2.9 Documento de Definição de Requisitos (DDR)

1. Introdução

   (a) Objetivo do Documento de Definição de Requisitos
   O presente documento tem por objetivo compilar os requisitos levantados para o Sistema de Gestão de Riscos de Investimentos em TI – SGRITI, dispondo das informações essenciais ao desenvolvimento do mesmo.

   - Definições, Acrônimos e Abreviações
     Os termos utilizados na padronização das especificações seguem como des-

critos a seguir.

RF (Requisito Funcional): São funções que o sistema deve oferecer [39].

RD (Requisito de Dados): São os dados necessários para programar as funcionalidades do sistema [13].

RNF (Requisito Não-Funcional): Descrevem uma restrição no sistema [39].

RE (Regra de Execução): São condições e padrões que devem ser seguidos para execução de um Requisito Funcional [13].

(b) Formatação

O formato das siglas para especificação dos requisitos obedecerá ao seguinte padrão: [Identificação do tipo de requisito] + [numeração sequencial a partir do 01].

Ex: RE01.

(c) Relacionamento entre requisitos

Para cada RF é obrigatório que haja pelo menos 01 (um) RD correspondente e, cada RF pode ter relacionado a ele, nenhuma ou várias RE.

2. Requisitos funcionais (RF)

(a) Manter fornecedor

Tabela 5.20: Manter fornecedor

Identificador	**RF**	**RD**	**RE**	**Prioridade**
RF01	Incluir fornecedor	RD01	RE05 RE06 RE08	Baixa
RF02	Editar fornecedor	RD02	RE05 RE06	Baixa
RF03	Excluir fornecedor	RD03	RE09	Baixa
RF04	Consultar fornecedor	RD04	RE07	Baixa

(b) Manter usuário

Tabela 5.21: Manter usuário

Identificador	**RF**	**RD**	**RE**	**Prioridade**
RF05	Incluir usuário	RD05	RE01 RE04 RE05	Média
RF06	Editar usuário	RD06	RE01 RE05	Média
RF07	Excluir usuário	RD07	RE03	Média
RF08	Consultar usuário	RD08	RE02	Baixa

(c) Manter ativo de TI

Tabela 5.22: Manter ativo de TI

Identificador	**RF**	**RD**	**RE**	**Prioridade**
RF09	Incluir ativo de TI	RD09	RE05 RE10 RE11	Alta
RF10	Editar ativo de TI	RD10	RE05 RE10	Alta
RF11	Excluir ativo de TI	RD11	RE12	Alta
RF12	Consultar ativo de TI	RD12	RE13	Alta

(d) Manter questionário

Tabela 5.23: Manter questionário

Identificador	**RF**	**RD**	**RE**	**Prioridade**
RF13	Incluir questionário	RD13	RE05 RE19 RE20	Alta
RF14	Editar questionário	RD14	RE05 RE19	Alta
RF15	Excluir questionário	RD15	RE22	Alta
RF16	Consultar questionário	RD16	RE21	Alta

(e) Manter critérios

Tabela 5.24: Manter critérios

Identificador	RF	RD	RE	Prioridade
RF17	Incluir critério	RD17	RE05 RE14 RE15 RE16	Alta
RF18	Editar critério	RD18	RE05 RE12	Alta
RF19	Excluir critério	RD19	RE17	Alta
RF20	Consultar critério	RD20	RE14	Alta

(f) Calcular pesos dos critérios

Tabela 5.25: Calcular pesos dos critérios

Identificador	RF	RD	RE	Prioridade
RF21	Definir critérios de análise de risco	RD21	RE23	Alta
RF22	Geração de uma matriz quadrad para inserção da análise par a par dos critérios	RD22	RE24	Alta
RF23	Geração do cálculo do peso que cada critério possui	RD23	RE25	Alta

(g) Efetuar análise de risco de ativos por critério

Tabela 5.26: Efetuar análise de risco de ativos por critério

Identificador	RF	RD	RE	Prioridade
RF24	Realizar análise de risco por ativos definidos	RD24	RE26 RE27	Alta
RF25	Gerar relatório de ativos de TI priorizados por risco de investimento	RD25	RE28	Alta
RF26	Gerar relatório detalhado de ativos por critério analisado	RD26	RE29	Alta

(h) Preencher questionário

Tabela 5.27: Preencher questionário

Identificador	**RF**	**RD**	**RE**	**Prioridade**
RF27	Vincular questionário a usuário convidado	RD27	RE30	Baixa
RF28	Enviar mensagem de acesso ao questionário	RD28	RE31	Baixa
RF29	Responder questionário	RD29	RE32	Baixa

3. Requisitos de dados (RD) Para cada requisito de dado deve ser preenchido com o nome do atributo e, cada atributo deve ter selecionado uma ou mais características. Estas características podem ser:

   - Obrigatório (O) - Atributo de preenchimento obrigatório.
   - Seleção (S) - Atributo selecionável, lista de múltipla escolha ou seleção única.
   - Editável (E) - Atributo editável que permite o preenchimento.
   - Leitura (L) - Atributo somente de leitura.

   Estes requisitos podem ser dos seguintes tipos:

   - Alfanumérico
   - Numérico
   - Caractere
   - Data

(a) Requisitos de Dados do RF01 - Incluir fornecedor

Tabela 5.28: Requisitos de Dados do RF01 - Incluir fornecedor

Nome	**O**	**S**	**E**	**L**	**Descrição**	**Exemplo**	**Tipo**
Nome fantasia	X		X		Nome fantasia da empresa	Tech-no	Alfanumérico
Razão social	X		X		Razão social do fornecedor	Tech-No Indústria e Comércio Ltda	Alfanumérico
CNPJ	X		X		CNPJ do fornecedor	54.823.999/0007-21	Numérico
E-mail	X		X		E-mail do fornecedor	tech@email.com	Alfanumérico
Endereço			X		Endereço do fornecedor	Av. das Castanheiras, 854, Águas Claras, DF	Alfanumérico
Telefone		X			Telefone do fornecedor	(61) 3333-1111	Numérico
Contato	X		X		Contato no forneccedor	Maria da Silva	Caractere

(b) Requisitos de Dados do RF02 - Editar fornecedor

Tabela 5.29: Requisitos de Dados do RF02 - Editar fornecedor

Nome	**O**	**S**	**E**	**L**	**Descrição**	**Exemplo**	**Tipo**
Código	X			X	Identificador do fornecedor	33	Numérico
Nome Fantasia	X		X		Nome fantasia da empresa	Tech-No	Alfanumérico
Razão Social	X		X		Razão social do fornecedor	Tech-No Indústria e Comércio Ltda	Alfanumérico
CNPJ	X	X			CNPJ do fornecedor	54.823.999/0007-21	Numérico
E-mail	X		X		E-mail do fornecedor	tech@email.com	Alfanumérico
Endereço			X		Endereço do fornecedor	Av. das Castanheiras, 854, Águas Claras, DF	Alfanumérico
Telefone		X			Telefone do fornecedor	(61) 3333-1111	Numérico
Contato	X		X		Contato no forneccedor	Maria da Silva	Caractere

(c) Requisitos de Dados do RF03 - Excluir fornecedor

Tabela 5.30: Requisitos de Dados do RF03 - Excluir fornecedor

Nome	**O**	**S**	**E**	**L**	**Descrição**	**Exemplo**	**Tipo**
Código	X			X	Identificador do fornecedor	33	Numérico
Nome Fantasia	X		X		Nome fantasia da empresa	Tech-No	Alfanumérico

(d) Requisitos de Dados do RF04 - Consultar fornecedor

Tabela 5.31: Requisitos de Dados do RF04 - Consultar fornecedor

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Nome Fantasia	X		X		Nome fantasia da empresa	Tech-No	Alfanumérico
Razão Social	X		X		Razão social do fornecedor	Tech-No Indústria e Comércio Ltda	Alfanumérico
CNPJ	X	X			CNPJ do fornecedor	54.823.999/0007-21	Numérico
E-mail	X		X		E-mail do fornecedor	tech@email.com	Alfanumérico

(e) Requisitos de Dados do RF05 - Incluir usuário

Tabela 5.32: Requisitos de Dados do RF05 - Incluir usuário

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Nome completo	X		X		Nome do usuário	Carlos Maurício de Borges Mello	Alfanumérico
CPF	X		X		CPF do fornecedor	060.260.758-28	Numérico
E-mail	X		X		E-mail do usuário	cmbmello@email.com	Alfanumérico
Telefone			X		Número do telefone	(61) 4321-1234	Numérico
Perfil	X	X			Perfil de acesso ao sistema	Administrador	Caractere

(f) Requisitos de Dados do RF06 - Editar usuário

Tabela 5.33: Requisitos de Dados do RF06 - Editar usuário

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Código	X			X	Identificador do fornecedor	33	Numérico
Nome completo	X		X		Nome do usuário	Carlos Maurício de Borges Mello	Alfanumérico
CPF	X		X		CPF do fornecedor	060.260.758-28	Numérico
E-mail	X		X		E-mail do usuário	cmbmello@email.com	Alfanumérico
Telefone			X		Número do telefone	(61) 4321-1234	Numérico
Perfil	X	X			Perfil de acesso ao sistema	Administrador	Caractere

(g) Requisitos de Dados do RF07 - Excluir usuário

Tabela 5.34: Requisitos de Dados do RF07 - Excluir usuário

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Código	X			X	Identificador do fornecedor	33	Numérico
CPF	X		X		CPF do fornecedor	060.260.758-28	Numérico

(h) Requisitos de Dados do RF08 - Consultar usuário

Tabela 5.35: Requisitos de Dados do RF08 - Consultar usuário

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Nome completo	X		X		Nome do usuário	José da Silva	Alfanumérico
CPF	X		X		CPF do fornecedor	060.260.758-28	Numérico
E-mail	X		X		E-maisl do usuário	cmbmello@email.com	

(i) Requisitos de Dados do RF09 - Incluir ativo

Tabela 5.36: Requisitos de Dados do RF09 - Incluir ativo

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Nome	X		X		Nome do ativo	DELL PE R710	Alfanumérico
Descrição	X		X		Descrição do ativo	Servidor com dois processadores Intel Xeon	Alfanumérico
Fabricante	X		X		Nome do Fabricante	DELL Computadores	Alfanumérico
Preço	X		X		Preço de referência	10.000,00	Numérico

(j) Requisitos de Dados do RF10 - Editar Ativo

Tabela 5.37: Requisitos de Dados do RF10 - Editar Ativo

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Código	X			X	Identificador do ativo	133	
Nome	X		X		Nome do ativo	DELL PE R710	Alfanumérico
Descrição	X		X		Descrição do ativo	Servidor com dois processadores Intel Xeon	Alfanumérico
Fabricante	X		X		Nome do Fabricante	DELL Computadores	Alfanumérico
Preço	X		X		Preço de referência	10.000,00	Numérico

(k) Requisitos de Dados do RF11 - Excluir ativo

Tabela 5.38: Requisitos de Dados do RF11 - Excluir ativo

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Código	X			X	Identificador do ativo	133	Numérico
Nome	X		X		Nome do ativo	DELL PE R710	Alfanumérico

(l) Requisitos de Dados do RF12 - Consultar ativo

Tabela 5.39: Requisitos de Dados do RF12 - Consultar ativo

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Nome	X		X		Nome do ativo	DELL PE R710	Alfanumérico
Descrição	X		X		Descrição do ativo	Servidor com dois processadores Intel Xeon	Alfanumérico
Fabricante	X		X		Nome do fabricante	DELL Computadores	Alfanumérico
Preço	X		X		Preço de referência	10.000,00	Numérico

(m) Requisitos de Dados do RF13 - Incluir questionário

Tabela 5.40: Requisitos de Dados do RF13 - Incluir questionário

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Nome	X		X		Nome do questionário	Questionário - Teste	Alfanumérico
Descrição	X		X		Descrição do questionário	Questionário para levantamento de Fator de Risco Operacional	Alfanumérico
Pergunta(s)	X		X		Pergunta(s) realizadas	Numa escala de 1 a 5, assinale a importância do ativo	Alfanumérico
Resposta(s)	X		X		Resposta(s) às perguntas	5 - Muito alta	Alfanumérico
Usuário	X		X		Usuário que respondeu o questionário	José da Silva	Alfanumérico

(n) Requisitos de Dados do RF14 - Editar questionário

Tabela 5.41: Requisitos de Dados do RF14 - Editar questionário

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Código	X			X	Identificador do questionário	33	Numérico
Nome	X		X		Nome do questionário	Questionário - Teste	Alfanumérico
Descrição	X		X		Descrição do questionário	Questionário para levantamento de Fator de Risco Operacional	Alfanumérico
Pergunta(s)	X		X		Pergunta(s) realizadas	Numa escala de 1 a 5, assinale a importância do ativo	Alfanumérico
Resposta(s)	X		X		Resposta(s) às perguntas	5 - Muito alta	Alfanumérico
Usuário	X		X		Usuário que respondeu o questionário	José da Silva	Alfanumérico

(o) Requisitos de Dados do RF15 - Excluir questionário

Tabela 5.42: Requisitos de Dados do RF15 - Excluir questionário

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Código	X			X	Identificador do questionário	33	Numérico
Nome	X		X		Nome do questionário	Questionário - Teste	Alfanumérico

(p) Requisitos de Dados do RF16 - Consultar questionário

Tabela 5.43: Requisitos de Dados do RF16 - Consultar questionário

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Nome	X		X		Nome do questionário	Questionário - Teste	Alfanumérico
Descrição	X		X		Descrição do questionário	Questionário para levantamento de Fator de Risco Operacional	Alfanumérico
Usuário	X		X		Usuário que respondeu o questionário	José da Silva	Alfanumérico

(q) Requisitos de Dados do RF17 - Incluir critério

Tabela 5.44: Requisitos de Dados do RF17 - Incluir critério

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Descrição	X		X		Descrição do critério	Preço atendimento "Per call"	Alfanumérico
Composição	X		X		Composição do critério	"Fórmula de cálculo do critério"	Alfanumérico
Relação	X		X		Relação do critério com a AR	Direta	Alfanumérico

(r) Requisitos de Dados do RF18 - Editar critério

Tabela 5.45: Requisitos de Dados do RF18 - Editar critério

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Código	X			X	Identificador do critério	33	Numérico
Descrição	X		X		Descrição do critério	Preço atendimento "Per call"	Alfanumérico
Composição	X		X		Composição do critério	"Fórmula de cálculo do critério"	Alfanumérico
Relação	X		X		Relação do critério com a AR	Direta	Alfanumérico

(s) Requisitos de Dados do RF19 - Excluir critério

Tabela 5.46: Requisitos de Dados do RF19 - Excluir critério

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Código	X			X	Identificador do critério	33	Numérico
Descrição	X		X		Descrição do critério	Preço atendimento "Per call"	Alfanumérico

(t) Requisitos de Dados do RF20 - Consultar critério

Tabela 5.47: Requisitos de Dados do RF20 - Consultar critério

Nome	O	S	E	L	Descrição	Exemplo	Tipo
Código	X			X	Identificador do critério	33	Numérico
Descrição	X		X		Descrição do critério	Preço atendimento "Per call"	Alfanumérico
Composição	X		X		Composição do critério	"Fórmula de cálculo do critério"	Alfanumérico

4. Regras de execução (RE)

Neste item serão descritos as regras de execução, descrições e os respectivos requisitos funcionais onde elas serão aplicadas.

Tabela 5.48: Regras de execução (RE01 até RE04)

Id	Descrição	RF
RE01	Não deve ser permitido que haja mais de um usuário com o mesmo login	RF05 RF06
RE02	A consulta poderá ser realizada pelos seguintes campos: Login, Perfil.	RF08
RE03	Caso o usuário já tenha realizado alguma operação no sistema, sua exclusão deverá ser apenas lógica, alterando seu status para 0 - Inativo.	RF07
RE04	Será gerado um número sequencial de 1 a N, que representará o usuário no sistema	RF05

Tabela 5.49: Regras de execução (RE05 até RE20)

Id	Descrição	RF
RE05	O sistema não deverá permitir que campos obrigatórios fiquem em branco.	RF01 RF02 RF05 RF06 RF09 RF10 RF15 RF16 RF17 RF18
RE06	Não deve ser permitida a duplicidade de CNPJ	RF01 RF02
RE07	A consulta poderá ser realizada pelos campos CNPJ e Nome Fantasia	RF04
RE08	Será gerado um número sequencial de 1 a N, que representará o fornecedor no sistema	RF01
RE09	Caso haja algum registro do fornecedor no sistema, sua exclusão deverá ser apenas lógica, alterando seu status para 0 - Inativo.	RF07
RE10	Não deve ser permitida a duplicidade de nome dos ativos.	RF09 RF10
RE11	Será gerado um número sequencial de 1 a N, que representará o ativo no sistema.	RF09
RE12	Caso haja algum registro do ativo no sistema, sua exclusão será permitida e, o botão de exclusão deve aparecer desativado.	RF11
RE13	A consulta deverá ser feita pelo nome do ativo.	RF12
RE14	Os critérios não poderão ultrapassar o número de 13, dentro do status 1-ativo.	RF17
RE15	Não deve ser permitido que haja duplicidade nos nomes dos ativos.	RF17 RF18
RE16	Será gerado um número sequencial de 1 a N, que representará o ativo no sistema.	RF17
RE17	Caso haja algum registro do ativo no sistema, sua exclusão deverá ser apena lógica, alterando seu status para 0 - Inativo..	RF19
RE18	A consulta deverá ser feita pelo nome do critério.	RF20
RE19	Não deve ser permitido que haja duplicidade nos nomes dos questionários.	RF13 RF14
RE20	Será gerado um número sequencial de 1 a N, que representará o questionário no sistema.	RF13

Tabela 5.50: Regras de execução (RE21 até RE32)

Id	Descrição	RF
RE21	A consulta deverá ser feita pelo nome do questionário.	RF16
RE22	Caso haja algum usuário já tenha respondido ao questionário, não deverá ser possível excluí-lo.	RF15
RE23	Devem ser selecionados no mínimo 02(dois) critérios para análise do risco	RF21
RE24	Gerar uma matriz quadrada para análise baseada na quantidade de critérios definidos.	RF22
RE25	Proceder o preenchimento da matriz de análise conforme descrito.	RF23
RE26	Realiza a análise par a par dos ativos de TI, tomando por base um único critério. Tal procedimento deve se repetir para todos os critérios selecionados para a análise.	RF24
RE27	O sistema deve montar uma matriz quadrada com os ativos de TI que devem ser comparados, semelhante à matriz gerada para os critérios.	RF24
RE28	Gerar um relatório baseado nas regras de negócio RE26 e RE27, levando em conta o risco por investimento.	RF25
RE29	Gerar um relatório detalhando todos os ativos relacionados, em cada um dos critérios utilizados para análise, conforme RE26 e RE27.	RF26
RE30	Podem ser selecionado um ou mais usuários convidados para responder o questionário.	RF27
RE31	A mensagem deve ser enviada através do email pré-cadastrado.	RF28
RE32	O questionário respondido pelo usuário convidado deve ter suas respostas enviadas ao mesmo como forma de confirmação.	RF29

Através do uso da metodologia de levantamento de requisitos iRON [13] e, com o foco no negócio existente, foram levantados os requisitos funcionais, de dados e regras de execução mínimas para o futuro desenvolvimento de um produto que possa atender às demandas de análise de risco em investimentos de TI no âmbito do DSIC do GSI/PR. No capítulo seguinte, será apresentado um estudo de caso que apresentará uma simulação da metodologia proposta, em um universo limitado do Departamento.

Capítulo 6

Apresentação do Modelo de Análise de Riscos Proposto: Estudo de Caso no DSIC

Após a conclusão das atividades de especificação de critérios de análise de riscos e de especificação dos requisitos de uma provável ferramenta, será apresentado agora, uma simulação de análise de riscos num universo restrito.
Para a realização desta atividade foram selecionados critérios da análise de riscos e ativos de TI do Departamento.
Os critérios identificados e catalogados no item 5.2.6 são específicos para análises de risco com foco na área financeira e, para essa simulação foram selecionados quatro deles por apresentarem uma visibilidade maior para o estudo. Assim, os critérios escolhidos foram os seguintes:

- preço de atendimento “per call”;
- preço global do produto;
- fator de risco operacional;
- tempo de vida útil.

O DSIC possui uma infraestrutura crítica composta por dezenas de ativos de TI. Para a realização desta simulação, foram escolhidos, aleatoriamente, um conjunto de ativos, que representam um universo reduzido, que englobam equipamentos de segurança física, segurança lógica e de processamento de dados.
O universo escolhido foi uma parcela da infraestrutura de TI do DSIC. Para essa simulação, foram escolhidos quatro critérios somente, pois mais critérios fariam com que a quantidade de cálculos aumentasse significativamente, e este pesquisador entende que

essa quantidade é suficientemente satisfatória para ilustrar a viabilidade técnica da metodologia proposta.
Dentro do patrimônio de TI do DSIC, foram selecionados os seguintes ativos de TI:

- Ativo 01: Modular Safe LMS 9.3;
- Ativo 02: UTM Aker Firewall Box;
- Ativo 03: Firewall de Aplicação WAF;
- Ativo 04: Servidor Dell PowerEdge R710.

Com o intuito de subsidiar a análise de riscos dos ativos de TI, foram coletadas algumas informações específicas da infraestrutura do DSIC, conforme detalhamento abaixo.
Para fim desse estudo, ainda, o valor declarado do patrimônio de TI do DSIC foi estimado em R$ 2.267.766,40 (dois milhões, duzentos e sessenta e sete mil, setecentos e sessenta e seis reais e quarenta centavos).
Os dados necessários para utilização do modelo proposto para os ativos de TI, podem ser vistos na tabela 6.1, a seguir:

Tabela 6.1: Estudo de Caso: Dados dos Ativos de TI para Cálculo dos Critérios

Atributo	**Ativo 01**	**Ativo 02**	**Ativo 03**	**Ativo 04**
% do Patrimônio:	18%	5%	2%	3%
Preço Global do Produto:	R$ 405.679,00	R$ 105.000,00	R$ 50.000,00	R$ 68.997,00
Quantidade Existente:	02 UN	02 UN	01 UN	03 UN
Preço Unitário	R$ 202.839,50	R$ 52.500,00	R$ 50.000,00	R$ 22.999,00
Tempo de vida útil	Indefinido	10 anos	10 anos	08 anos
Tempo de vida restante	Indefinido	09 anos	07 anos	02 anos
Valor anual do contrato	R$ 90.180,72	R$ 50.661,60	R$ 42.954,05	R$ 11.963,88
Valor anual do contrato individualizado	R$ 45.090,36	R$ 25.330,80	R$ 42.954,05	R$ 3.987,96
Valor atendimento "Per call"	R$ 11.300,00	R$ 7.500,00	R$ 18.500,00	R$ 2.500,00

6.1 Construção da estrutura de decisão hierárquica

A figura 6.1, apresenta a estrutura desejada para o nosso estudo de caso.

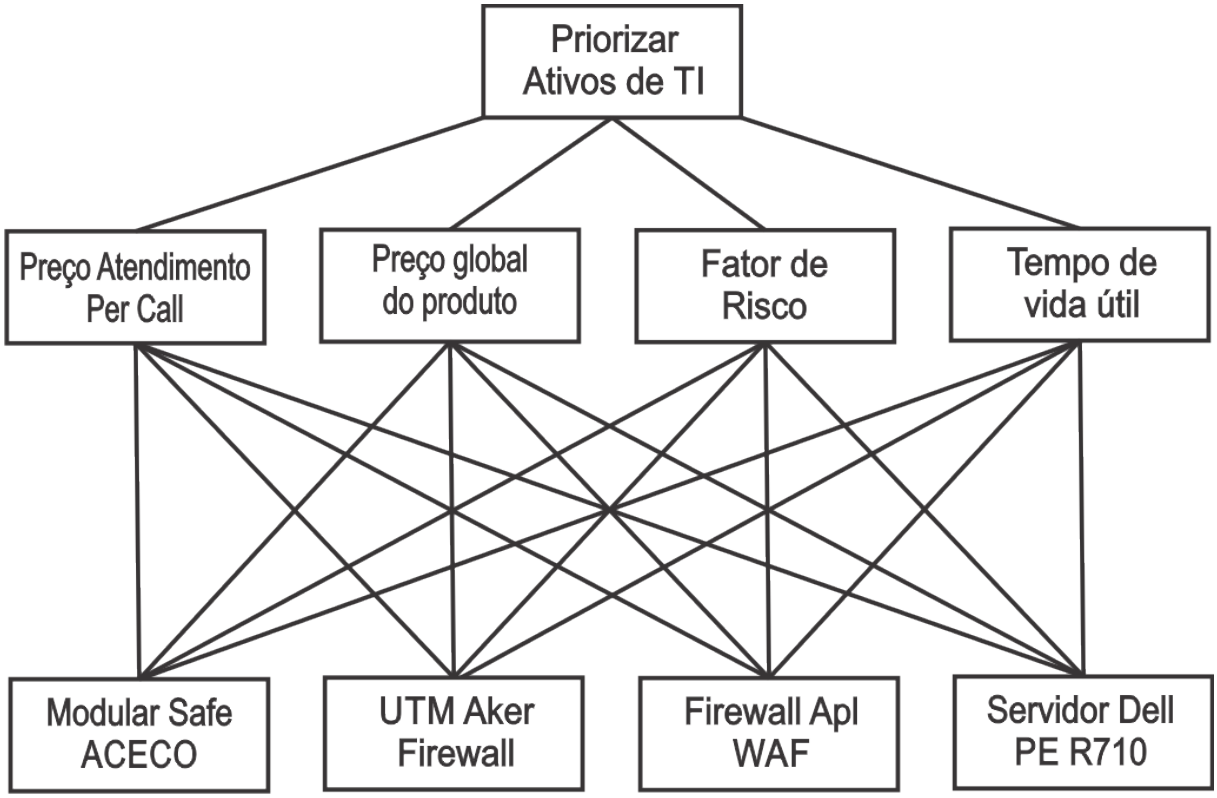

Figura 6.1: Estudo de caso: Estrutura de decisão hierárquica .

Esse organograma apresenta a estrutura de decisão hierárquica. Nesse caso, em particular, optou-se por fazer apenas um nível de hierarquia. Assim, pode-se perceber, no topo da estrutura, o objetivo do método, sendo apresentado logo a seguir, os critérios de mesmo nível e, por último os ativos de TI que serão analisados pelos critérios elencados.

6.2 Construção das matrizes de comparação entre critérios

A partir da montagem da hierarquia, os critérios precisam ser avaliados par a par, a fim de se determinar a importância relativa entre eles e seu peso relativo no objetivo final. Dessa forma a avaliação se inicia pela determinação do peso relativo dos grupos de critérios iniciais. A tabela a seguir apresenta os dados de peso relativo entre os critérios, que foi determinado pelos tomadores de decisão do DSIC.

O critério considerado mais importante pelos analistas do departamento foi o risco, por-

que, na sua composição, estabeleceu-se parâmetros inerentes aos serviços prestados. Partindo da premissa de que o foco principal de qualquer órgão da APF é o negócio, ou produto finalístico, há um consenso generalizado de que o fator de risco tem relevância sobre todos os demais critérios.

Ao utilizar o fator de risco operacional como referência, foi feita uma análise par a par dos critérios. Inicialmente comparou-se risco com os demais critérios e, após isso, uma comparação entre pares dos demais critérios. O resultado dessas comparações pode ser visto na figura 6.2.

Os valores utilizados são aqueles especificados pela Escala de Saaty [33], que utiliza valores compreendidos entre 1 e 9, inclusive. No entanto, para auxiliar e otimizar os cálculos necessários, utilizou-se o Microsoft Excel 2013, que automaticamente converte as frações, dando maior visibilidade à aplicação da metodologia, por valores decimais.

O "Fator de Risco" foi considerado o critério mais importante dentre aqueles selecionados para compor o processo de análise e, assim, a construção dessa matriz iniciou-se com a comparação par a par desse critério com os demais. Será apresentado agora um resumo das comparações realizadas desse critério, com os demais.

Fator de Risco versus Preço global do produto: peso 6. Nessa comparação o critério fator de risco apresenta importância absoluta em relação ao Preço global. Assim, também, uma pequena diferença, semelhante à análise anterior, esse par de critérios apresenta uma diferença um pouco mais acentuada a favor do critério fator de risco.

Fator de Risco versus Preço atendimento "per call": peso 2, pois há uma pequena importância desse critério sobre o Preço atendimento "per call". Os valores desses atendimentos tendem a impactar o orçamento do órgão, então, esses dois critérios apresentam referências muito semelhantes, com pouca distinção entre si, com ligeiro favorecimento ao critério fator de risco.

Fator de Risco versus Tempo de Vida Útil: peso 3. Apesar de haver, também, uma pequena diferença, semelhante à análise anterior, esse par de critérios apresenta uma diferença um pouco mais acentuada a favor do critério risco.

As demais comparações foram todas realizadas, buscando a coerência estabelecida nessa primeira rodada de comparações, e a figura 6.2, ficou assim preenchida:

	Preço atendimento “per call”	Preço global do Produto	Fator de Risco	Tempo de vida útil
Preço atendimento “per call”	1,00	0,33	0,50	0,67
Preço global do Produto	3,00	1,00	0,33	2,00
Fator de Risco	2,00	6,00	1,00	3,00
Tempo de Vida Útil	1,50	0,50	0,33	1,00

Figura 6.2: Estudo de Caso: Matriz comparativa do grupo de critérios .

Os valores foram convertidos em decimais, tendo em vista a utilização da planilha eletrônica do Microsoft Excel.

O passo seguinte foi a normalização da matriz comparativa, procedimento que permite a interpretação e atribuição de pesos relativos a cada critério.

A normalização é feita pela divisão entre cada valor da planilha com o total de cada coluna, apresentado na linha “Soma”. Os valores normalizados podem ser vistos na parte inferior da figura 6.3, especificamente, abaixo da linha “Soma”).

	Preço atendimento Per call	Preço global do Produto	Fator de Risco	Tempo de vida útil
Preço atendimento Per call	1,00	0,33	0,50	0,67
Preço global do Produto	3,00	1,00	0,33	2,00
Fator de Risco	2,00	6,00	1,00	3,00
Tempo de vida útil	1,50	0,50	0,33	1,00
Soma	7,50	7,83	2,17	6,67
	Preço atendimento Per call	Preço global do Produto	Fator de Risco	Tempo de vida útil
Preço atendimento Per call	0,13	0,04	0,23	0,10
Preço global do Produto	0,40	0,13	0,15	0,30
Fator de Risco	0,27	0,77	0,46	0,45
Tempo de vida útil	0,20	0,06	0,15	0,15

Figura 6.3: Estudo de caso: Matriz comparativa normalizada do grupo de critérios .

A determinação da contribuição que cada critério provê no objetivo proposto é calculada a partir do vetor de prioridade ou vetor de Eigen.
O vetor de Eigen apresenta os pesos relativos entre os critérios e é obtido de modo aproximado, pois cálculos exatos devem ser feitos somente para casos específicos.
O cálculo, então, é feito através da média aritmética dos valores de cada um dos critérios, conforme apresentado na figura 6.4.

	Preço atendimento Per call	Preço global do Produto	Fator de Risco	Tempo de vida útil	Média Vetor de Eigen
Preço atendimento Per call	0,13	0,04	0,23	0,10	0,127
Preço global do Produto	0,40	0,13	0,15	0,30	0,245
Fator de Risco	0,27	0,77	0,46	0,45	0,486
Tempo de vida útil	0,20	0,06	0,15	0,15	0,142

Figura 6.4: Estudo de caso: Cálculo do vetor de Eigen .

Uma forma de verificar se os cálculos estão corretos, é realizar o somatório dos valores do vetor (Coluna “Média”), que sempre deve totalizar 1 (um).
A importância desse cálculo deve-se ao fato de que ele determina a participação, ou melhor, o peso de cada critério no resultado final do estudo.
Para validar esses cálculos, é necessária à verificação da Inconsistência dos dados. Isso significa identificar se os tomadores de decisão do DSIC foram consistentes em suas opiniões durante este processo, ou seja, se os valores atribuídos em cada comparação (par a par) foram coerentes durante a análise de todos os pares disponíveis na matriz. Assim, quanto maior for a inconsistência da matriz de decisão, maiores disparidades serão apresentadas entre os resultados obtidos pelo cálculo do vetor de prioridades. Uma matriz é considerada consistente, quando esse cálculo é menor que 10Para realizar este cálculo, utilizou-se a ferramenta Expert Choice, que no caso apresentado, ficou em 0,02, conforme pode ser visto no detalhe destacado na figura 6.5.

	Preço_Percall	Preço global	Fator de Risco	Tempo de vida útil
Preço_Percall		3,0	2,0	1,0
Preço global			6,0	2,0
Fator de Risco				3,0
Tempo de vida útil	Incon: 0,02			

Figura 6.5: Estudo de caso: Tela do Expert choice (Teste de consistência) .

A figura 6.6, apresenta agora, a mesma estrutura de decisão hierárquica visualizada anteriormente, mas com a adição do peso que cada critério tem sobre a análise de riscos como um todo.

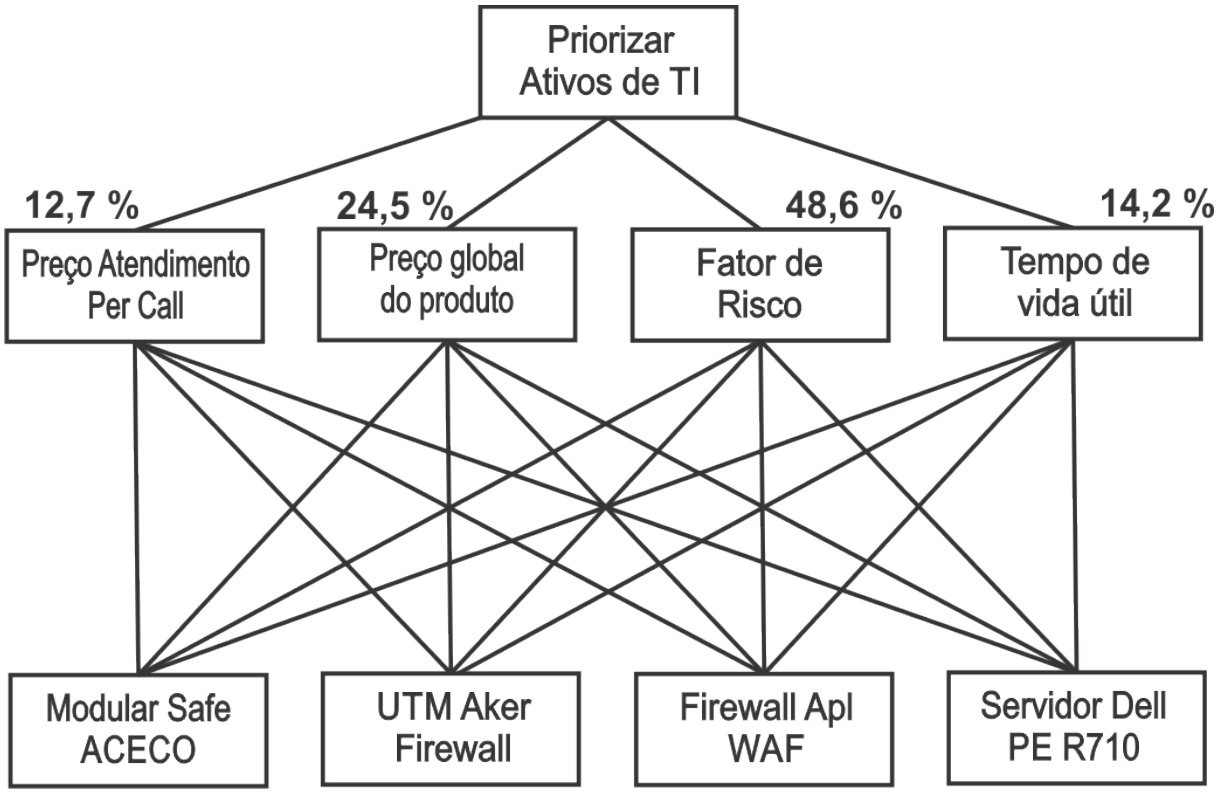

Figura 6.6: Estudo de caso: Estrutura de decisão hierárquica (com peso por critério) .

6.3 Construção das matrizes de comparação dos ativos por critérios

Uma vez que a estrutura de decisão hierárquica esteja definida e os pesos dos critérios estabelecidos, é possível, agora, determinar como cada critério vai impactar no universo de ativos selecionados para a análise.

Os ativos serão agora comparados par a par, considerando agora, de forma isolada, cada um dos critérios estabelecidos.

No presente estudo de caso, foram identificados quatro ativos diferentes que necessitam ser priorizados.

6.3.1 Matriz comparativa dos ativos no critério preço de atendimento “per call”

Para a análise dos ativos nesse critério, é necessário realizar os cálculos estabelecidos no item 5.2.6 (p.:75), bem como a efetiva aplicação dos indicadores lá estabelecidos.
A figura a seguir apresenta o resumo dos cálculos realizados, bem como o enquadramento dos ativos nos indicadores estabelecidos:

Preço atendimento Per call	Valor do Contrato (R$)	Valor do Contrato Individual (R$)	Preço Atendimento "per call" (R$)	% do Preço Atendimento "per call"	Indicador atribuído
Modular Safe LMS 9.3	90.180,72	45.090,36	11.300,00	0,25	2
UTM Aker Firewall Box	50.661,60	25.330,80	7.500,00	0,30	2
Firewall de aplicação WAF	42.954,05	42.954,05	18.500,00	0,43	4
Servidor Dell PowerEdge R710	11.963,88	3.987,96	2.500,00	0,63	6

Figura 6.7: Estudo de caso: Enquadramento dos ativos nos indicadores do critério Preço de atendimento “per call” .

Após essa etapa, a matriz de comparação dos ativos para esse critério pode ser visualizada na figura 6.8.

Preço atendimento Per call	Modular Safe LMS 9.3	UTM Aker Firewall Box	Firewall de aplicação WAF	Servidor Dell PowerEdge R710
Modular Safe LMS 9.3	1,00	1,00	0,50	0,33
UTM Aker Firewall Box	1,00	1,00	0,50	0,33
Firewall de aplicação WAF	2,00	2,00	1,00	0,67
Servidor Dell PowerEdge R710	3,00	3,00	1,50	1,00

Figura 6.8: Estudo de caso: Matriz comparativa dos ativos no critério Preço de atendimento “per call” .

As figuras seguintes, 6.9 e 6.10 apresentam o desdobramento dos cálculos da normalização e da média, que são necessários para completar a análise dos ativos sob a óptica desse critério.

Preço atendimento Per call	Modular Safe LMS 9.3	UTM Aker Firewall Box	Firewall de aplicação WAF	Servidor Dell PowerEdge R710
Modular Safe LMS 9.3	1,00	1,00	0,50	0,33
UTM Aker Firewall Box	1,00	1,00	0,50	0,33
Firewall de aplicação WAF	2,00	2,00	1,00	0,67
Servidor Dell PowerEdge R710	3,00	3,00	1,50	1,00
Soma	7,00	7,00	3,50	2,33
Preço atendimento Per call	Modular Safe LMS 9.3	UTM Aker Firewall Box	Firewall de aplicação WAF	Servidor Dell PowerEdge R710
Modular Safe LMS 9.3	0,14	0,14	0,14	0,14
UTM Aker Firewall Box	0,14	0,14	0,14	0,14
Firewall de aplicação WAF	0,29	0,29	0,29	0,29
Servidor Dell PowerEdge R710	0,43	0,43	0,43	0,43

Figura 6.9: Estudo de caso: Matriz comparativa normalizada dos ativos no critério Preço de atendimento “per call” .

Preço atendimento Per call	Modular Safe LMS 9.3	UTM Aker Firewall Box	Firewall de aplicação WAF	Servidor Dell PowerEdge R710	Média
Modular Safe LMS 9.3	0,14	0,14	0,14	0,14	0,14
UTM Aker Firewall Box	0,14	0,14	0,14	0,14	0,14
Firewall de aplicação WAF	0,29	0,29	0,29	0,29	0,29
Servidor Dell PowerEdge R710	0,43	0,43	0,43	0,43	0,43

Figura 6.10: Estudo de caso: Cálculo da média dos ativos no critério Preço de atendimento "per call" .

A partir deste ponto, o processo torna-se repetitivo para os cálculos dos três critérios restantes, pois seguem o mesmo padrão apresentado e, sendo assim, serão apresentados apenas os cálculos para o estabelecimento dos seus indicadores, as médias obtidas e, por fim o cálculo final com a obtenção da prioridade esperada na metodologia proposta.

6.3.2 Matriz comparativa dos ativos no critério "preço global do produto"

O critério "preço global do produto", conforme detalhado na no item 5.2.6 (p.:77), utiliza valores diretamente proporcionais ao valor total do patrimônio de TI estimado do órgão. Para fins da simulação da metodologia, o valor do patrimônio de TI do DSIC foi estimado em R$ 2.267.766,40 (dois milhões, duzentos e sessenta e sete mil, setecentos e sessenta e seis reais e quarenta centavos). A figura 6.11 apresenta o resumo dos cálculos realizados, bem como o enquadramento dos ativos nos indicadores estabelecidos e, a figura 6.12, o resultado final para esse critério.

Preço Global do Produto	Preço Global do Produto	Valor do Patrimônio de TI	% do Preço global do produto	Indicador atribuído
Modular Safe LMS 9.3	R$ 405.679,00	R$ 2.267.766,40	0,18	1
UTM Aker Firewall Box	R$ 105.000,00	R$ 2.267.766,40	0,05	1
Firewall de aplicação WAF	R$ 50.000,00	R$ 2.267.766,40	0,02	1
Servidor Dell PowerEdge R710	R$ 68.997,00	R$ 2.267.766,40	0,03	1

Figura 6.11: Estudo de caso: Enquadramento dos ativos nos indicadores do critério Preço global do produto .

Preço Global do Produto	Modular Safe LMS 9.3	UTM Aker Firewall Box	Firewall de aplicação WAF	Servidor Dell PowerEdge R710	Média
Modular Safe LMS 9.3	0,25	0,25	0,25	0,25	0,25
UTM Aker Firewall Box	0,25	0,25	0,25	0,25	0,25
Firewall de aplicação WAF	0,25	0,25	0,25	0,25	0,25
Servidor Dell PowerEdge R710	0,25	0,25	0,25	0,25	0,25

Figura 6.12: Estudo de caso: Cálculo da média dos ativos no critério Preço global do produto .

6.3.3 Matriz comparativa dos ativos no critério "Fator de risco operacional"

O critério "fator de risco operacional", conforme detalhado no item 5.2.6 (p.:81), utiliza valores calculados a partir da multiplicação de três fatores internos: probabilidade, severidade e relevância.

A figura 6.13 apresenta o resumo dos cálculos realizados, bem como o enquadramento dos ativos nos indicadores estabelecidos e, a figura 6.14, o resultado final para esse critério.

Fator de Risco	Probabilidade	Severidade	Relevância	Cálculo do Risco	Indicador atribuído
Modular Safe LMS 9.3	3	5	5	75	9
UTM Aker Firewall Box	3	4	3	36	6
Firewall de aplicação WAF	2	2	3	12	3
Servidor Dell PowerEdge R710	2	2	3	12	3

Figura 6.13: Estudo de caso: Enquadramento dos ativos nos indicadores do critério "Fator de risco operacional" .

Fator de Risco	Modular Safe LMS 9.3	UTM Aker Firewall Box	Firewall de aplicação WAF	Servidor Dell PowerEdge R710	Média
Modular Safe LMS 9.3	0,43	0,43	0,43	0,43	0,43
UTM Aker Firewall Box	0,29	0,29	0,29	0,29	0,29
Firewall de aplicação WAF	0,14	0,14	0,14	0,14	0,14
Servidor Dell PowerEdge R710	0,14	0,14	0,14	0,14	0,14

Figura 6.14: Estudo de caso: Cálculo da média dos ativos no critério "Fator de risco operacional" .

6.3.4 Matriz comparativa dos ativos no critério "tempo de vida útil"

O critério "tempo de vida útil", conforme detalhado no item 5.2.6 (p.:79), é estimado a partir do quociente da divisão do tempo de uso pelo tempo de vida útil total do ativo. Quando o item não possuir tempo de vida útil (total ou remanescente) disponível, será usado o valor 1 (um). O valor a ser utilizado é o tempo remanescente, então sempre se calcula o complemento a 100%, dos valores obtidos na divisão acima mencionada. A figura 6.15 apresenta o resumo dos cálculos realizados, bem como o enquadramento dos ativos nos indicadores estabelecidos e, a figura 6.16, o resultado final para esse critério.

Tempo de vida útil	Tempo de uso	Tempo de Vida útil	% Tempo de vida útil Remanescente	Indicador Atribuído
Modular Safe LMS 9.3	1	1	0,00	1
UTM Aker Firewall Box	1	10	0,90	2
Firewall de aplicação WAF	3	10	0,70	4
Servidor Dell PowerEdge R710	6	8	0,25	8

Figura 6.15: Estudo de caso: Enquadramento dos ativos nos indicadores do critério Tempo de vida útil remanescente .

Tempo de vida útil	Modular Safe LMS 9.3	UTM Aker Firewall Box	Firewall de aplicação WAF	Servidor Dell PowerEdge R710	Média
Modular Safe LMS 9.3	0,07	0,07	0,07	0,07	0,07
UTM Aker Firewall Box	0,13	0,13	0,13	0,13	0,13
Firewall de aplicação WAF	0,27	0,27	0,27	0,27	0,27
Servidor Dell PowerEdge R710	0,53	0,53	0,53	0,53	0,53

Figura 6.16: Estudo de caso: Cálculo da média dos ativos no critério Tempo de vida útil remanescente .

6.3.5 Cálculo do Indicador Final de Prioridades da Análise de Risco

Uma vez que todas as matrizes foram calculadas, normalizadas e suas respectivas médias obtidas, a última etapa será realizar os cálculos finais que apontarão um valor percentual que, quando ordenado de forma decrescente, indicará a ordem de prioridades com que os ativos de tecnologia da informação devem ser observados para aplicação de investimentos. A seguir é apresentada a sequência de eventos necessária para a realização dos cálculos que permitirão a obtenção do resultado final.

Cada ativo possui uma média específica calculada de acordo com cada critério selecionado (vide figura 6.17) e, cada critério possui um valor médio calculado pelo Vetor de Eigen

(vide figura 6.18).
O cálculo deve ser realizado da seguinte forma: para cada ativo, deve-se somar os produtos de suas médias observadas em cada critério, pela média do critério obtida no Vetor de Eigen. Esse cálculo é detalhado na figura 6.19.

Resumo das Médias – Por ativo de TI	Preço atendimento Per call	Preço global do Produto	Fator de Risco	Tempo de vida útil
	Média	Média	Média	Média
Modular Safe LMS 9.3	0,14	0,25	0,43	0,07
UTM Aker Firewall Box	0,14	0,25	0,29	0,13
Firewall de aplicação WAF	0,29	0,25	0,14	0,27
Servidor Dell PowerEdge R710	0,43	0,25	0,14	0,53

Figura 6.17: Estudo de caso: Síntese das médias dos ativos por critério .

Média Vetor de Eigen	
Preço atendimento Per call	0,127
Preço global do Produto	0,245
Fator de Risco	0,486
Tempo de vida útil	0,142

Figura 6.18: Estudo de caso: Síntese Vetor de Eigen .

	Preço atendimento Per call	Preço global do Produto	Fator de Risco	Tempo de vida útil	Resultado
Modular Safe LMS 9.3	(0,14*0,127) +	(0,25*0,245) +	(0,43*0,486) +	(0,07*0,142)	29,72%
UTM Aker Firewall Box	(0,14*0,127) +	(0,25*0,245) +	(0,29*0,486) +	(0,13*0,142)	23,72%
Firewall de aplicação WAF	(0,29*0,127) +	(0,25*0,245) +	(0,14*0,486) +	(0,27*0,142)	20,48%
Servidor Dell PowerEdge R710	(0,43*0,127) +	(0,25*0,245) +	(0,14*0,486) +	(0,53*0,142)	26,08%

Figura 6.19: Estudo de caso: Cálculos finais do método proposto .

Com todos os valores obtidos nos itens anteriores e consolidados, conforme ilustrado na figura 6.19, pode-se, agora, transportar os resultados finais para a estrutura de decisão hierárquica e apresentada graficamente na figura 6.20:

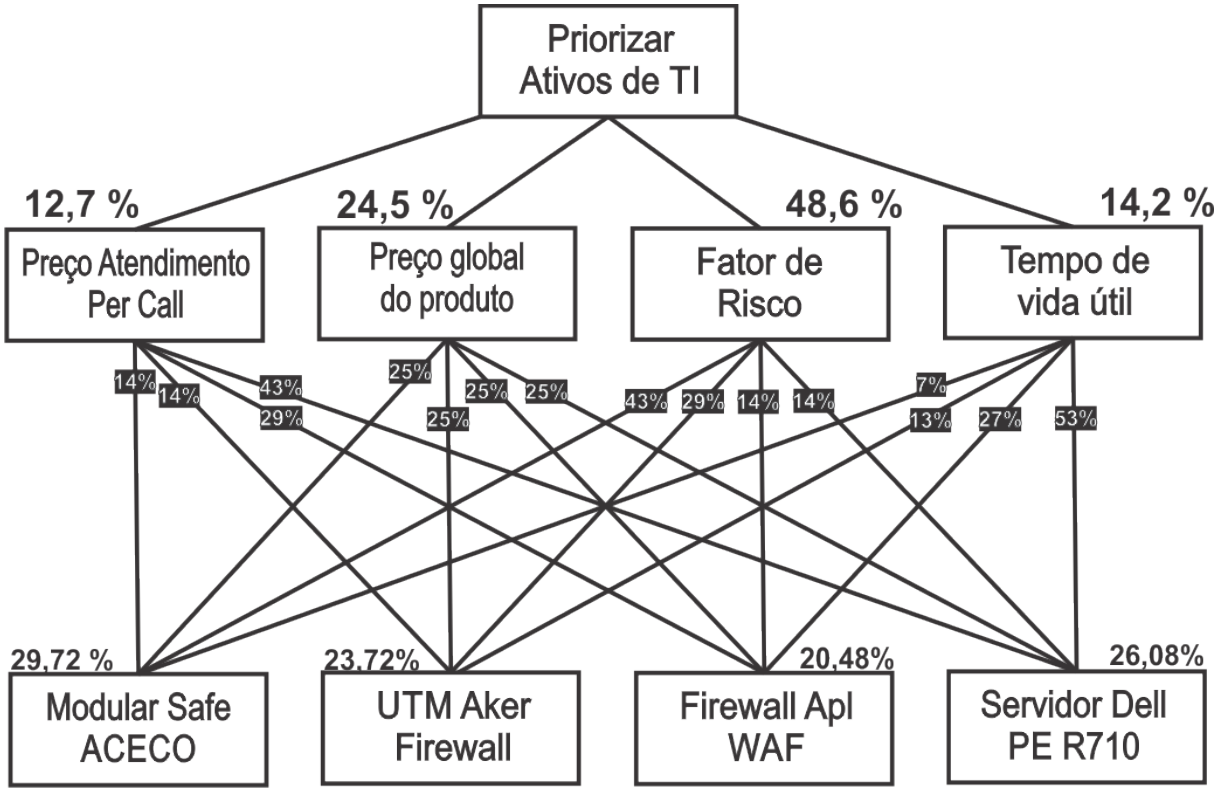

Figura 6.20: Estudo de caso: Estrutura de decisão hierárquica – Resultados finais .

6.3.6 Análise dos resultados do Estudo de Caso

Com o término da sequência de cálculos, pode-se verificar os seguintes detalhes:
Cada critério, isoladamente, apresenta uma lista de prioridades independentes. Sendo assim, isoladamente, teríamos os seguintes resultados:

- Se o conjunto de ativos fosse analisado somente sob o ponto de vista do critério: Preço de Atendimento "per call":

  1. Servidor Dell PowerEdge R710, com 43% (quarenta e três por cento);
  2. Firewall Apl WAF, com 29% (vinte e nove por cento);
  3. Modular Safe, da ACECO, com 14% (quatorze por cento); e
  4. UTM Aker Firewall, com 14% (quatorze por cento).

- Se o conjunto de ativos fosse analisado somente sob o ponto de vista do critério: Preço Global do Produto":

  1. Modular Safe, da ACECO, com 25% (vinte e cinco por cento);
  2. UTM Aker Firewall, com 25% (vinte e cinco por cento);
  3. Firewall Apl WAF, com 25% (vinte e cinco por cento); e
  4. Servidor Dell PowerEdge R710, com 25% (vinte e cinco por cento).

  Note-se que nesse critério não haveria prioridade. A escolha desse critério foi apenas para demonstrar que em alguns casos, um único critério pode não ser suficiente para a metodologia proposta.

- Se o conjunto de ativos fosse analisado somente sob o ponto de vista do critério: Tempo de Vida Útil:

  1. Modular Safe, da ACECO, com 43% (quarenta e três por cento);
  2. UTM Aker Firewall, com 29% (vinte e nove por cento).
  3. Firewall Apl WAF, com 14% (quatorze por cento); e
  4. Servidor Dell PowerEdge R710, com 14% (quatorze por cento).

- Se o conjunto de ativos fosse analisado somente sob o ponto de vista do critério: Fator de Risco Operacional:

  1. Servidor Dell PowerEdge R710, com 53
  2. Firewall Apl WAF, com 27

3. UTM Aker Firewall, com 13
4. Modular Safe, da ACECO, com 07

Por outro lado, se ao invés de usar um único critério para auxílio na tomada de decisão na seleção de ativos, fossem utilizados todos os critérios disponíveis, o resultado final da simulação seria o seguinte:

1. Modular Safe, da ACECO, com 29,72% (vinte e nove vírgula setenta e dois por cento);
2. UTM Aker Firewall, com 23,72% (vinte e três vírgula setenta e dois por cento);
3. Servidor Dell PowerEdge R710, com 26,08% (vinte e seis vírgula zero oito por cento); e
4. Firewall Apl WAF, com 20,48% (vinte vírgula quarenta e oito por cento).

Através da utilização do método AHP, que combina múltiplos critérios para auxiliar o processo decisório, o resultado obtido, não foi feito por intermédio de um processo arbitrário, ou mesmo aleatório, mas sim, através de um procedimento racional e compreensivo onde um determinado problema de decisão foi, convenientemente modelado, sendo possível quantificar todas as variáveis envolvidas, num processo hierárquico de critérios que foram devidamente ponderados pelo gestor e, que resultaram num modelo que permitiu analisar várias alternativas, vários cenários de forma rápida e metódica, justificando, assim, uma decisão.
Isto posto, nessa simulação, os resultados indicam que o ativo de TI com maior prioridade de investimentos seria o do grupo de ativos de TI "Modular Safe ACECO", pois esse grupo apresentou o maior percentual, enquanto que o grupo de ativos de TI "Firewall Apl WAF" teria a menor prioridade, tendo em vista ser o item com o menor percentual consolidado.
Dessa forma, pode-se considerar a simulação concluída, pois foi evidenciado, de forma concreta, que a análise de riscos através da utilização de múltiplos critérios específicos contribuiu, de forma metódica, prática e rápida para o estabelecimento de uma lista de prioridades para investimentos de tecnologia da informação.

Capítulo 7

Conlusão

Inicialmente, a pesquisa buscou identificar, através de pesquisas exploratórias as principais ferramentas de análise de riscos disponíveis no mercado mundial com o levantamento de um conjunto de ferramentas que foram classificadas em dois grupos distintos: um com foco em gestão de riscos e outro com foco em gestão de políticas e conformidades. As ferramentas de gestão de riscos foram exploradas de forma mais detalhada e, delas, foram elicitados um conjunto de requisitos considerados essenciais à construção de um software específico para análise de riscos para investimentos financeiros em tecnologia da informação.

Após essa fase, a empresa brasileira Modulo GRC, fabricante da ferramenta Modulo Risk Manager, disponibilizou equipamento, software e técnicos para auxiliar a pesquisa, na tentativa de verificar a possibilidade dessa ferramenta em alcançar o objetivo do contexto pesquisado. Após algumas semanas, concluiu-se que a ferramenta não teria condições de proceder a análise de riscos sob a óptica desejada e, assim, um novo objetivo foi desenvolvido.

Existe um pensamento geral em todas a ferramentas estudadas de pensar em vulnerabilidades e conformidades, quando se fala em análise de riscos.

Considerando a falta de um método ou de uma ferramenta que faça a análise de riscos para a tomada de decisão em investimentos financeiros de tecnologia da informação, a pesquisa passou então, na identificação de um conjunto de critérios específicos para a análise de riscos desejada. Os critérios identificados foram obtidos através de pesquisas e reuniões com técnicos das áreas de tecnologia, de licitações e de orçamento e finanças do DSIC do GSI/PR, bem como do Exército Brasileiro.

Na etapa seguinte, foi feito um mapeamento do processo atual de contratação de TI, conhecido como “As Is”, onde o problema que originou a pesquisa ficou evidenciado, quer seja, a falta de um procedimento metodológico que auxiliasse o tomador de decisão na seleção dos ativos de TI a serem priorizados, no caso de recursos orçamentários limitados.

Ato contínuo, foi feito um estudo do processo atual e foi concebido um modelo otimizado na expectativa de resolver o problema destacado. Esse novo modelo, conhecido como modelo "To Be", apresentou um conjunto de modificações que auxiliaram a pesquisa no estabelecimento de requisitos funcionais para a especificação de uma nova ferramenta.
Vencida essa etapa, o trabalho se encerra com um estudo de caso, cuja finalidade foi a de demonstrar a aplicabilidade da metodologia proposta. Nesse capítulo, foram selecionados critérios e ativos de TI específicos para a simulação e, esta simulação apresentou todas as etapas do desenvolvimento do processo de hierarquização dos critérios, com o estabelecimento de pesos entre eles e, posterior análise dos ativos de TI selecionados.
O capítulo termina com a análise dos ativos de TI, critério por critério, demonstrando que isoladamente, cada critério poderia definir uma lista de prioridades diferentes e, que, quando combinados, o resultado seria fruto de procedimento racional, ponderado e, que consideraria todos os critérios, combinando-os através da modelagem de todo o processo de forma hierárquica, onde todas as variáveis envolvidas seriam consideradas e serviriam de subsídio para justificar o processo decisório, como um todo.
Isto posto, conclui-se que a metodologia proposta, com os critérios identificados, poderia ser colocada em prática, não só no DSIC, como em outro órgão da APF, mediante modificações e adaptações que se fizerem necessárias em decorrência do estabelecimento do contexto de cada órgão.
Esta pesquisa não tem a intenção de esgotar o assunto do contexto da pesquisa, mas acredita-se que seja suficientemente estruturada para prover aos gestores de TI elementos essenciais para análises de riscos de investimentos de TI, pois combina o risco tecnológico, através do critério "Fator de Risco Operacional" com os demais critérios cujos cunhos são essencialmente relacionado a investimentos.
A metodologia proposta pode ser aplicada, mesmo quando um órgão possui orçamento suficiente para o cumprimento de todo o seu plano de metas especificado e detalhado no PDTI do órgão e, nesse caso, ela serviria como instrumento para determinação de prioridades para investimentos financeiros de tecnologia da informação.

7.1 Sugestão de trabalhos e atividades futuras

1. Automatizar a metodologia apresentada através do desenvolvimento de um software específico;
2. Estender a pesquisa na busca de novos critérios que venham a corroborar com o tema proposto; e

3. Montar uma base de conhecimentos dos critérios e seus indicadores estabelecidos a fim de subsidiar futuros ajustes na utilização da metodologia por outros órgãos da APF.

Referências

[1] ABNT. *ABNT ISO GUIA 73 - Gestão de riscos - Vocabulário*. Associação Brasileira de Normas Técnicas, Rio de Janeiro, nov. 2009. 9

[2] ABNT. *ABNT NBR 31000 - Gestão de Riscos - Princípios e Diretrizes*. Associação Brasileira de Normas Técnicas, Rio de Janeiro, nov. 2009. xii, 9, 41

[3] Agiliance. Agiliance riskvision v7.0 (hf1). `http://www.agiliance.com/products/platform.html`. xii, 36, 37

[4] Inc Allgress. Allgress insight and risk manager v5. `http://www.allgress.com/en/products/risk-analysis-module/`. xii, 38, 39

[5] Misael Sousa de Araújo. Análise de maturidade da gestão de riscos de ti na fiocruz: definição e aplicação de instrumento de avaliação e especificação de requisitos para um sistema computacional. 2014. 12

[6] Departamento de Segurança da Informação e Comunicações Brasil. Nc 04/in01/dsic/gsipr – diretrizes para o processo de gestão de riscos de segurança da informação e comunicações – grsic nos órgãos e entidades da apf, 2009. 9

[7] Ministério da Fazenda. Secretaria de Tesouro Nacional Brasil. Manual de contabilidade aplicada ao setor público. 5a edição:16, julho 2012. 79

[8] Orçamento e Gestão Brasil, Ministério do Planejamento. Instrução normativa nr 04 – dispõe sobre o processo de contratação de soluções de tecnologia da informação pelos órgãos integrantes do sistema de administração de recursos de tecnologia da informação e informática (sisp) do poder executivo federal. 2014. xiii, 61, 97, 98, 99, 100, 101, 102

[9] Orçamento e Gestão Brasil, Ministério do Planejamento. Instrução normativa nr 05 – dispõe sobre os procedimentos administrativos básicos para a realização de pesquisa de preços para a aquisição de bens e contrataçãoo de serviços em geral. 2014. 86

[10] TCU Tribunal de Contas da União Brasil. Acórdão 1603/2008-plenário - levantamento acerca da governança de tecnologia da informação na administração pública federal. *Levantamento de auditoria*, 2008. 1

[11] TCU Tribunal de Contas da União Brasil. Acórdão 2308/2010-plenário - relatório de levantamento. avaliação da governançaa de tecnologia da informaçãoo na administração pública federal. constatação de precariedades e oportunidades de melhoria. determinações, recomendações e comunicações. *Relatório de Levantamento*, 2010. 2

[12] TCU Tribunal de Contas da União Brasil. Acórdão 2467/2013-plenário - levantamento de auditoria. elaboração de indicador para medir o grau de maturidade de entidades públicas na gestão de riscos. constatação de que, em média, as entidades estão em nível intermediário no gerenciamento de riscos. determinações à unidade técnica. autorização para divulgação das informações consolidadas e dos dados públicos coletados. *Levantamento de auditoria*, 2013. 2, 9, 24

[13] Roberto; Calazans Angélica; Guimarães Fernando Castro, Eduardo; Paldês. *Engenharia de Requisitos: Um enfoque prático na construção de software orientado a negócio*. Bookess, 2014. 64, 103, 117

[14] Idalberto Chiavenato. *Introdução à teoria geral da administração*. Elsevier Brasil, 2000. 12

[15] Robert Clemen and Terence Reilly. *Making hard decisions with DecisionTools*. Cengage Learning, 2013. 11

[16] eGestalt Technologies Inc. Aegify vmarch2014. `https://www.aegify.com/risk-management.html`. xii, xv, 34, 35

[17] Antonio Carlos Gil. *Métodos e técnicas de pesquisa social*. Atlas, 2010. 6

[18] Carlos Francisco Simões e de Almeida Adiel Teixeira Gomes, Luiz Flavio Autran Monteiro e Gomes. *Tomada de decisão gerencial: enfoque multicritério*. Atlas, 2009. 12

[19] André Gonçalves. Ieee std 830 prática recomendada para especificações de exigências de software. *FCUL – Universidade de Lisboa*, Abril 2004. 22

[20] Roger Hussey and Jill Collins. *Pesquisa em administração: um guia prático para alunos de graduação e pós-graduação*. Porto Alegre: Bookman, 2005. 6

[21] Institute of Electrical IEEE and Electronics Engineers. Ieee recommended practice for software requirements specifications. 22

[22] ISACA. Cobit 5: A business framework for the governance and management of enterprise it. *Rolling Meadows: ISACA*, 2012. 11

[23] Raphael Mandarino Junior. Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro. *CEGSIC/2009. Disponível em: http://dsic.planalto.gov.br/cegsic/83-monografias-da-1o-turma-do-cegsic*, 2009. 2, 3

[24] Walfrido Brito Magalhães, Ivan Luizio e Pinheiro. *Gerenciamento de Serviços de TI na Prática*. 2007. 1

[25] Acuity Risk Manager. Stream integrated risk manager. `http://www.acuity.com`. Accessed: 2014-09-20. xii, 31, 32, 33

[26] GRC Modulo. Módulo risk manager v8.4. `https://www.modulo.com.br/software`. xii, xiii, 40, 56, 57, 58, 59, 82, 83

[27] Gilberto de Oliveira Moritz and Mauricio Fernandes Pereira. *Processo decisório*. SEAD/UFSC, 2006. 12

[28] Paulo Hideo Ohtoshi. Análise comparativa de metodologias de gestão e de análise de riscos sob a Ótica da norma nbr iso/iec 27005. *Brasília: UNB*, 2008. 3

[29] Roger S Pressman. *Engenharia de software*. McGraw Hill Brasil, 2006. 64

[30] Alcimar Sanches Rangel. Estudo da metodologia de análise de riscos ebios para aplicação na administração pública federal: Potencial alinhamento à legislação brasileira. *Brasília: UNB*, 2010. 2, 3

[31] Lucas de Lima Rodrigues. Estudo de caso de gestão baseada em itil em uma organização para aplicação de modelo de referência. 2015. 11, 84

[32] Corporation Rsam. Rsam solution for governance risk and compliance platform v8.2. `http://www.rsam.com/solutions/rsam-grc.html`. xii, 42, 43, 44

[33] Thomas L Saaty. Método de análise hierárquica. *Método de análise hierárquica*, 1991. xv, 13, 14, 76, 77, 78, 80, 84, 85, 88, 121

[34] Thomas L Saaty. *Theory and applications of the analytic network process: decision making with benefits, opportunities, costs, and risks*. RWS publications, 2005. Disponível em: <`http://books.google.com.br/books?id=65N6FiNBMjEC&printsec=frontcover&hl=ptBR&source=gbs_ge_summary_r&cad=0`>. Acesso em: 25 jun. 2014. xii, xv, 14, 15

[35] Ms Claudia Rosana Felisberto Scofano, Erick de Franco Abraham, Leonardo de Souza Silva, and Marcelo Amaral Teixeira. Gestão de risco em projetos: Análise das etapas do pmi-pmbok (project management institute). 2013. 10

[36] Roterdan Moura da Silva. Métodos de decisão multicritério: Anp. *ITA*, 2005. 13, 15

[37] Herbert Alexander Simon. *A capacidade de decisão e de liderança*. USAID, 1963. 11

[38] Security Skybox. Skybox view enterprise suite 7.0. `http://www.skyboxsecurity.com/products/overview`. xii, 45, 46, 47

[39] Ian Sommerville. *Engenharia de Software, 8ª edição, Tradução: Selma Shin Shimizu Mel-nikoff, Reginaldo Arakaki, Edilson de Andrade Barbosa*. São Paulo: Pearson Addison-Wesley, 2007. 22, 103

[40] Peter Stephenson and SC Magazine. Mitigating risk is not as simple as it seems. *SC Magazine (June 2014). Disponível em: http://www.scmagazine.com/mitigating-risk-is-not-as-simple-as-it-seems/article/346194/*, 2014. xii, xv, 6, 24, 25, 28, 29, 30, 49

[41] Peter Stephenson and SC Magazine. Product information: Acuity stream integrated risk manager v3.1. *SC Magazine (June 2014). Disponível em: http://www.scmagazine.com/acuity-stream-integrated-risk-manager-v31/review/4188/*, 2014. 31

[42] Peter Stephenson and SC Magazine. Product information: Aegify vmarch2014. *SC Magazine (June 2014). Disponível em: http://www.scmagazine.com/aegify-vmarch2014/review/4194/*, 2014. 34

[43] Peter Stephenson and SC Magazine. Product information: Agiliance riskvision v7.0 (hf1). *SC Magazine (June 2014). Disponível em: http://www.scmagazine.com/agiliance-riskvision-v70-hf1/review/4189*, 2014. 35

[44] Peter Stephenson and SC Magazine. Product information: Allgress insight and risk manager v5. *SC Magazine (June 2014). Disponível em: http://www.scmagazine.com/allgress-insight-and-risk-manager-v5/review/4191*, 2014. 37

[45] Peter Stephenson and SC Magazine. Product information: Modulo risk manager v8.4. *SC Magazine (June 2014). Disponível em: http://www.scmagazine.com/modulo-risk-manager-v84/review/4197*, 2014. 39, 41

[46] Peter Stephenson and SC Magazine. Product information: Rsa archer grc platform 5.4 sp1. *SC Magazine (June 2014). Disponível em: http://www.scmagazine.com/rsa-archer-grc-platform-54-sp1/review/4201*, 2014. 41, 42

[47] Peter Stephenson and SC Magazine. Product information: Rsam grc platform v 8.2. *SC Magazine (June 2014). Disponível em: http://www.scmagazine.com/rsam-grc-platform-v-82/review/4202*, 2014. 42

[48] Peter Stephenson and SC Magazine. Product information: Skybox view enterprise suite v7.0. *SC Magazine (June 2014). Disponível em: http://www.scmagazine.com/skybox-view-enterprise-suite-v70/review/4203*, 2014. 44

[49] Peter Stephenson and SC Magazine. Product information: Trustedagent grc v5.0.4. *SC Magazine (June 2014). Disponível em: http://www.scmagazine.com/trustedagent-grc-v504/review/4204*, 2014. 47

[50] Integration Incorporated Trusted. Trustedagent grc v5.0.4. `http://www.trustedintegration.com/trustedagent-grc.html`. xii, 47, 48

Apêndice A

Elicitação de requisitos detalhado por ferramenta

Tabela 4.6: Elicitação de requisitos detalhado por ferramenta

	FERRAMENTA	FABRICANTE	PAÍS	SÍTIO	RESUMO	PRINCIPAIS FUNCIONALIDADES
1.	Acuity STREAM Integrated Risk Manager v3.1	Acuity Risk Management	UK	http://www.acuityrm.com	Ferramenta do tipo cliente-servidor, que é orientada a riscos, onde realiza monitoramento de conformidade, produção de relatórios.	- Estabelecimento do contexto - Cadastro de ativos - Cadastro de atributos de ativos - Customização da matriz de riscos - Exportar relatórios em planilhas - Importar relatório de planilhas - Suporte a Windows - Suporte a Linux - Integração com AD - Integração com LDAP
2.	Aegify vMarch2014	Aegify Technologies	USA	http://www.aegify.com/	Solução baseada em assinatura, tipo SaaS. Possui foco em gestão de postura de segurança e gestão de risco e conformidade.	- Estabelecimento do contexto - Cadastro de ativos - Cadastro de atributos de ativos - Suporte a Windows - Suporte a Linux não identificado - Integração com AD - Integração com LDAP não identificado
3.	Agiliance RiskVision v7.0 (HF1)	Agiliance	USA	http://www.agiliance.com/	Ferramenta pode ser do tipo cliente-servidor, ou baseada em nuvem, sob demanda. É focada em riscos e atua com consultoria constante, via software.	- Estabelecimento do contexto - Cadastro de ativos - Cadastro de atributos de ativos - Exportar relatórios em planilhas - Importar relatório de planilhas - Suporte a Windows - Integração com AD
4.	Allgress Insight and Risk Manager v5	Algress	USA	http://www.algress.com	Ferramenta do tipo cliente-servidor que atua na gestão de risco, podendo se integrar a soluções pré-existentes.	- Estabelecimento do contexto - Cadastro de ativos - Cadastro de atributos de ativos - Suporte a Windows - Suporte a Linux não identificado - Integração com AD não identificado - Integração com LDAP não identificado

	FERRAMENTA	FABRICANTE	PAÍS	SÍTIO	RESUMO	PRINCIPAIS FUNCIONALIDADES
5.	Modulo Risk Manager v8.4	Modulo	BR	https://www.modulo.com.br	Ferramenta do tipo cliente-servidor que automatize os processos de gestão de risco e conformidade. Como o próprio nome diz, a ferramenta atua em módulos que são completamente integráveis, entre si.	- Estabelecimento do contexto - Cadastro de ativos - Cadastro de atributos de ativos - Customização da matriz de riscos - Exportar relatórios em planilhas - Importar relatório de planilhas - Suporte a Windows - Integração com AD
6.	RSA Archer GRC Platform 5.4 SP1	RSA Archer	USA	http://www.emc.com	Ferramenta do tipo cliente-servidor que atua com gestão de riscos, gerenciando auditorias e avaliações de risco, de forma qualitativa ou quantitativa. Permite investigações, gestão da violação e gestão de crises.	- Estabelecimento do contexto - Cadastro de ativos - Exportar relatórios em planilhas - Importar relatório de planilhas - Suporte a Windows - Integração com AD
7.	Rsam GRC Platform v 8.2	Rsam	USA	http://www.rsam.com	Ferramenta do tipo cliente-servidor que atua no gerenciamento de riscos além de inteligência de risco de segurança (avaliação do risco, gestão de conformidade, de ameaças, vulnerabilidades, dentre outras.	- Estabelecimento do contexto - Cadastro de ativos - Cadastro de atributos de ativos - Exportar relatórios em planilhas - Importar relatório de planilhas - Suporte a Windows - Suporte a Linux não identificado - Integração com AD - Integração com LDAP não identificado
8.	Skybox View Enterprise Suite v7.0	Skybox Security	USA	http://www.skyboxsecurity.com	Ferramenta do tipo cliente-servidor que atua no controle de vulnerabilidades, gestão de ameaças, de políticas de firewall, de rede e gestão de mudanças.	- Estabelecimento do contexto - Cadastro de ativos - Suporte a Windows - Suporte a Linux - Integração com AD - Integração com LDAP

	FERRAMENTA	FABRICANTE	PAÍS	SÍTIO	RESUMO	PRINCIPAIS FUNCIONALIDADES
9.	TrustedAgent GRC V5.0.4	Trusted Integration	USA	http://www.trustedintegration.com	Ferramenta baseada em assinatura, tipo SaaS. Possui foco em gestão .de risco soba óptica da NIST SP 800-37	- Estabelecimento do contexto - Cadastro de ativos - Exportar relatórios em planilhas não identificado - Importar relatório de planilhas não identificado - Suporte a Windows - Suporte a Linux não identificado - Integração com AD - Integração com LDAP não identificado

Apêndice B

Mapeamento do processo de contratação de TI no DSIC (Fluxo atual)

Apêndice C

Mapeamento do processo de contratação de TI no DSIC (Fluxo proposto)